



Common Criteria for Information Technology Security Evaluation

CCEB-96/014

Part 4: Predefined Protection Profiles

Version 1.0

96/01/31

Foreword

Following extensive international cooperation to align the source criteria from Canada (CTCPEC), Europe (ITSEC) and the United States of America (TCSEC and Federal Criteria), version 1.0 of the *Common Criteria for Information Technology Security Evaluation* is issued for the purpose of trial evaluations and for review by the international security community. The practical experience acquired through trial evaluations and all the comments received will be used to further develop the criteria.

A template for reporting observations on version 1.0 of the CC is included at the end of this document. Any observation reports should be communicated to one or more of the following points of contact at the sponsoring organisations:

National Institute of Standards and Technology

Computer Security Division
NIST North Building, Room 426
Gaithersburg, Maryland 20899
U.S.A.
Tel: (+1)(301)975-2934, Fax:(+1)(301)926-2733
E-mail:csd@nist.gov
<http://csrc.ncsl.nist.gov>

National Security Agency

Attn: V2, Common Criteria Technical Advisor
Fort George G. Meade, Maryland 21122
U.S.A.
Tel: (+1)(410)859-4458, Fax:(+1)(410)684-7512
E-mail: common_criteria@radium.ncsc.mil

Communications Security Establishment

Criteria Coordinator
R2B IT Security Standards and Initiatives
P.O. Box 9703, Terminal
Ottawa, Canada K1G 3Z4
Tel:(+1)(613)991-7409, Fax:(+1)(613)991-7411
E-mail:criteria@cse.dnd.ca
<ftp:ftp.cse.dnd.ca>
<http://www.cse.dnd.ca>

UK IT Security and Certification Scheme

Senior Executive
P.O. Box 152
Cheltenham GL52 5UF
United Kingdom
Tel: (+44) 1242 235739, Fax:(+44)1242 235233
E-mail: ccv1.0@itsec.gov.uk
[ftp: ftp.itsec.gov.uk](ftp:ftp.itsec.gov.uk)
<http://www.itsec.gov.uk>

Bundesamt für Sicherheit in der Informationstechnik

Abteilung V
Postfach 20 03 63
D-53133 Bonn
Germany
Tel: (+49)228 9582 300, Fax:(+49)228 9582 427
E-mail:cc@bsi.de

**Service Central de la Sécurité des Systèmes
d'Information**

Bureau Normalisation, Critères Communs
18 rue du docteur Zamenhof
92131 Issy les Moulineaux
France
Tel: (+33)(1)41463784, Fax:(+33)(1)41463701
E-mail:ssi28@calvacom.fr

Netherlands National Communications Security Agency

P.O. Box 20061
NL 2500 EB The Hague
The Netherlands
Tel: (+31) 70 3485637, Fax:(+31).70.3486503
E-mail: criteria@nlncsa.minbuza.nl

Table of contents

Chapter 1		
	Introduction	1
1.1	Scope	1
1.2	Status of Part 4	1
1.3	Organisation of Part 4	2
1.4	Protection Profile overview	2
1.5	Plans for progress of the Protection Profiles	3
 Chapter 2		
	Commercial Security 1 (CS1) Protection Profile	5
2.1	Introduction	5
2.1.1	Identification	5
2.1.2	Protection Profile overview	5
2.2	TOE description	5
2.3	Security environment	6
2.3.1	Summary	6
2.3.2	Threats to security	6
2.3.3	Organisational security policies	8
2.3.4	Secure usage assumptions	9
2.4	Security objectives	10
2.4.1	IT security objectives	10
2.4.2	Non-IT security objectives	11
2.5	TOE IT security requirements	11
2.5.1	Functional requirements	12
2.5.2	Assurance requirements	17
2.6	Environmental IT security requirements	17
2.7	Application notes	17
 Chapter 3		
	Commercial Security 3 (CS3) Protection Profile	21
3.1	Introduction	21
3.1.1	Identification	21
3.1.2	Protection Profile overview	21
3.2	TOE description	22
3.3	Security environment	23
3.3.1	Summary	23
3.3.2	Secure usage assumptions	23
3.3.3	Organisational security policies	24
3.3.4	Threats to security	25
3.4	Security objectives	29
3.4.1	IT security objectives	29
3.4.2	Non-IT security objectives	30
3.5	TOE IT security requirements	30
3.5.1	Functional requirements	30

3.5.2	Assurance requirements	54
3.6	Environmental IT security requirements	55
3.7	Application notes	56

Chapter 4

	Network/Transport Layer Packet Filter Firewall (PFFW) PP	57
4.1	Introduction	57
4.1.1	Identification	57
4.1.2	Protection Profile overview	57
4.2	TOE description	57
4.3	Security environment	58
4.3.1	Summary	58
4.3.2	Threats to security	58
4.3.3	Organisational security policies	61
4.3.4	Secure usage assumptions	61
4.4	Security objectives	62
4.4.1	IT security objectives	62
4.4.2	Non-IT security objectives	63
4.5	TOE IT security requirements	64
4.5.1	Functional requirements	64
4.5.2	Assurance requirements	72
4.6	Environmental IT security requirements	72
4.7	Application notes	72

Annex A

	Rationale for CS1 Protection Profile	75
A.1	Introduction	75
A.2	CS1 Security objectives	75
A.2.1	Threats to be addressed by the TOE	75
A.2.2	Threats to be addressed by the operating environment	77
A.2.3	Satisfaction of policies	77
A.2.4	Completeness of objectives	78
A.3	CS1 Functional requirements rationale	79
A.4	CS1 Functional requirements dependencies	89
A.5	CS1 Assurance requirements rationale	90
A.6	Mapping to FC/CS1 requirements	90
A.6.1	Mapping to FC/CS1 functional requirements	90
A.6.2	Mapping to FC/CS1 assurance requirements	96

Annex B

	Rationale for CS3 Protection Profile	103
B.1	Introduction	103
B.2	CS3 Security objectives	103
B.2.1	Satisfaction of organisational security policies	103
B.2.2	Threats to be addressed by the TOE	104
B.2.3	Threats to be addressed by the operating environment	107
B.2.4	Completeness of objectives	108

B.3	CS3 Functional requirements rationale	109
B.3.1	Identification and authentication requirements rationale	110
B.3.2	TOE access requirements rationale	114
B.3.3	Trusted path requirements rationale	117
B.3.4	User data protection requirements rationale	118
B.3.5	Audit requirements rationale	121
B.3.6	Protection of TSF requirements rationale	129
B.3.7	Resource utilisation requirements rationale	134
B.4	Satisfaction of IT security objectives	135
B.5	CS3 Functional requirements dependencies	136
B.6	CS3 Assurance requirements rationale	140
B.6.1	Evaluation assurance level rationale	140
B.6.2	Assurance augmentations rationale	140

Annex C

Rationale for PFFW Protection Profile 143

C.1	Introduction	143
C.2	PFFW Security objectives	143
C.2.1	Threats to be addressed by the TOE	143
C.2.2	Threats to be addressed by the operating environment	147
C.2.3	Policies to be addressed by the TOE	148
C.2.4	Completeness of the objectives	148
C.3	PFFW Functional requirements	150
C.4	PFFW Assurance requirements	160

Annex D

CC observation report (CCOR) 161

D.1	Introduction	161
D.2	Categorisation of observation report	161
D.3	Format of observation report	162
D.3.1	Tag definitions for observation report	162
D.3.2	Example observations:	164
D.4	Printed observation report	165

List of figures

Figure 4.1 - Typical firewall location in a network environment	58
Figure 4.2 - Allowed and disallowed connections for compliant firewalls	62

List of tables

Table 2.1 -	Functional components of CC/CS1	12
Table 3.1 -	CS3 functional requirements	31
Table 3.2 -	CS3 assurance requirements	54
Table 4.1 -	Functional Components	64
Table 4.2 -	Auditable events	66
Table A.1 -	Mapping of security objectives to threats and policies	78
Table A.2 -	Functional component dependency analysis	89
Table A.3 -	Mapping to FC/CS1 functional requirements	91
Table A.4 -	Mapping to FC/CS1 assurance requirements	96
Table B.1 -	Mapping objectives to threats and organisational security policies	108
Table B.2 -	Mapping objectives to functional requirements	135
Table B.3 -	CS3 functional component dependency analysis	137
Table B.4 -	CS3 assurance requirements	140
Table C.1 -	Mapping of threats to security objectives	145
Table C.3 -	Mapping of security objectives to threats	149
Table C.4 -	Functional components included in this PP	150
Table D.1 -	CC observation report	166

Chapter 1

Introduction

1.1 Scope

- 1 Part 4 contains the Protection Profiles (PPs) that are part of the Common Criteria (CC) version 1.0. The PPs included in this version of Part 4 are presented partly as the basis for trial evaluations against CC version 1.0 and partly as worked examples of the concepts in the CC.
- 2 Three PPs have been included in this version. Two PPs have been created from the source criteria which form the historical input to the CC, and one has been developed for a type of IT product which is new to the process of security evaluation.

1.2 Status of Part 4

- 3 The profiles presented in this issue of Part 4 of the Common Criteria (CC) are published as examples for comment and trial use. They have been developed by the authors of the CC as part of the process of validating the CC technical approach and the specific security requirements contained in the CC.
- 4 At the time of publication, these profiles have not been evaluated using the relevant CC criteria. Such evaluations are planned to take place during the trial period of the CC. Until such evaluations have been completed successfully and the profiles have been registered for general use, these profiles must be treated as provisional.
- 5 CC profiles CS1 and CS3 represent further development of the Federal Criteria profiles CS1 and CS3 expressed using the CC approach and terminology. It is important to note that no attempt has been made to achieve exact equivalency. Differences in the granularity and content of the CC components as compared to the Federal Criteria requirements make it difficult to reconstruct previous profiles precisely. The CC CS1 profile is intended to be an acceptable substitute for the Federal Criteria profile CS1 (and hence TCSEC C2) but is not identical to these sets of requirements. The CC CS3 profile is intended to meet the same consumer needs as the Federal Criteria CS3 whilst incorporating the findings of further research into role based access control security policies.
- 6 The CC Firewall profile is the first member of a possible family of related Firewall profiles and represents a trial application of the CC to products which are of interest to the security community but have not been well matched to previous evaluation criteria.
- 7 Readers should note that, whilst the CC recommends a high level PP structure and mandates the content of such a structure, it makes no statement about the detailed

presentational approach. The presentations of the CC Part 4 profiles should be considered as exemplary. PP authors are invited to investigate alternate presentational approaches in the interests of improved readability. Other presentational approaches may be preferable provided that the CC content requirements are complied with and the evaluation requirements are met.

1.3 Organisation of Part 4

- 8 Chapter 1 is the introductory material for Part 4.
- 9 Chapter 2 is the PP for Commercial Security 1 (CS1) - Basic Controlled Access Protection. CS1 is equivalent to Federal Criteria CS1 and consists of TCSEC C2 security requirements plus those evaluation interpretations that a product must meet before it can be rated at the C2 level.
- 10 Chapter 3 is the PP for Commercial Security 3 (CS3) - Role-Based Access Protection. CS3 was originally specified in the Federal Criteria and has been updated for this version of the CC based on more recent research. CS3 specifies a strong set of security functions and assurances for general purpose multi-user operating systems, database management systems, and other applications in sensitive environments. CS3 supports a variety of organisation specific non-discretionary integrity and confidentiality policies calling for access controls based on individual roles of users with respect to data objects and permitted operations.
- 11 Chapter 4 is the PP for a Network/Transport Packet Filter Firewall (PFFW). This PP has not been derived from previous criteria and specifies security functions and assurances applicable to most commercially available packet filter firewalls. The PP reflects current market practices for this type of product, rather than mandating novel approaches.
- 12 Annexes A through C respectively contain the rationale for each of the three PPs. These rationale statements are considered to be of primary value as PP evaluation deliverables by providing the basis for the selection of the security objectives and the functional and assurance requirements.
- 13 Annex D contains the instructions for reporting observations and problems to the authors.

1.4 Protection Profile overview

- 14 The PP is a CC construct which allows users to describe re-usable sets of security requirements of proven utility. All of the source criteria contain some sets of standardised requirements for functions and assurance. The PP brings those two types of requirements together with a statement of the security problem that a compliant product is intended to solve, so that prospective users can determine its applicability to specific uses. Although the PP concept has been borrowed from the Federal Criteria, it has its conceptual origin in the TCSEC digraphs and its structural origin in the ITSEC security target.

- 15 Each PP consists of the following key parts:
- a) The security environment is a narrative statement of the security problem to be solved by a TOE compliant to the PP. The environment is described in terms of anticipated threats in such an environment, security policies to be enforced, and usage assumptions about the TOE.
 - b) The security objectives are a set of statements that summarises the security problem to be solved and are the basis for definition of the requirements.
 - c) Functional requirements are components from Part 2 (refined as necessary to meet specific needs by applying certain operations described in Part 2). Assurance requirements consist of an Evaluation Assurance Level from Part 3, augmented as necessary to meet specific needs by addition of assurance components from Part 3.
 - d) An additional part of the PP is the rationale, which is evaluation evidence to demonstrate that the relationship between the requirements and objectives exists and is valid.
- 16 Part 1 describes the relationship of the PP with other CC constructs such as the Security Target (ST) and Target of Evaluation (TOE). Annex B of Part 1 contains the detailed structural requirements for PPs. The PPs contained in this Part 4 are compliant with the requirements of that annex.

1.5 Plans for progress of the Protection Profiles

- 17 It is expected that Part 4 will evolve into a registry of PPs that have been developed, evaluated, and accepted for use by the participating evaluation schemes.

Chapter 2

Commercial Security 1 (CS1) Protection Profile

2.1 Introduction

2.1.1 Identification

18 Title: Commercial Security 1 (CS1) - Basic Controlled Access Protection.

19 Registration: <To be filled in upon registration>

20 Keywords: Access control, discretionary access control, general-purpose operating system, information protection

2.1.2 Protection Profile overview

21 CC CS1 uses the CC requirements components to model the CS1 profile from the Federal Criteria (FC). The FC CS1 was developed to directly correspond to the TCSEC C2 as it had come to be interpreted at the time of FC publication.

22 CS1 specifies a baseline set of security functions and assurances for workstations, general-purpose multi-user operating systems, database management systems, and other applications. CS1 compliant products support access controls that are capable of enforcing access limitations on individual users and data objects.

23 CS1 provides for a level of protection which is appropriate for an assumed non-hostile and well managed user community which requires protection against threats of inadvertent or casual attempts to breach the system security. CS1 is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well resourced attackers, whether authorised users or not, to breach system security. CS1 compliant products are suitable for use in both commercial and government environments.

24 CS1 is generally applicable to distributed IT systems but does not address the security requirements which arise specifically out of the need to distribute the IT resources within a network.

2.2 TOE description

25 CS1 defines a set of security requirements to be levied on Targets of Evaluation (TOEs) which include workstations, general purpose operating systems, and applications. Such TOEs permit one or more processors and attached peripheral and storage devices to be used by multiple users to perform a variety of functions requiring controlled shared access to the data stored on the system. Such installations are typical of personal, workgroup, or enterprise computing systems

accessed by users local to, or with otherwise protected access to, the computer systems.

- 26 CS1 is applicable to TOEs that provide facilities for on-line interaction with users. CS1 is also generally applicable to TOEs incorporating network functions but contains no network specific requirements. Networking is covered only to the extent to which the TOE can be considered to be part of a centrally-managed system that meets a common set of security requirements.
- 27 CS1 assumes that responsibility for the safeguarding of the data protected by the TOE can be delegated to the TOE users. All data is under the control of the TOE. The data is stored in named objects, and the TOE can associate with each controlled object a description of the access rights to that object.
- 28 All individual users are assigned a unique user identifier. This user identifier supports individual accountability. The TOE authenticates the claimed identity of the user before allowing the user to perform any further actions.
- 29 A CS1 compliant TOE enforces controls such that access to data objects can only take place in accordance with the access restrictions placed on that object by its owner or other suitably authorised user.
- 30 Access rights (e.g. read, write, execute) can be assigned to data objects with respect to subjects (e.g. users). Once a subject is granted access to an object, the content of that object may be freely used to influence other accessible objects.

2.3 Security environment

2.3.1 Summary

- 31 This section identifies the security issues which govern the choice of the CS1 security requirements. It identifies the threats to the data security which the CS1 requirements are intended to counter, security policies for which CS1 compliant TOEs are appropriate, and the physical, personnel and other aspects of the environment of the TOE.

2.3.2 Threats to security

- 32 CS1 compliant TOEs are required to counter threats which may be broadly categorised as the threat of attack from hostile outsiders with no legitimate access to the system, and threats from insiders with legitimate access to the system attempting to gain access to and perform operations on objects for which they have no individually defined rights. In addition, certain threats of a non-IT nature can affect the security of CS1 compliant TOEs and must be dealt with by the operating environment.

2.3.2.1 Threats addressed by TOE

- 33 The threat possibilities discussed below are addressed by CS1 compliant TOEs:

T.ACCESS An unauthorised person may gain logical access to the TOE.

34 The term unauthorised person is used to cover all those persons who have, or may attempt to gain, physical access to the system and its terminals but have no authority to gain logical access to its resources.

35 It is assumed that such unauthorised persons could possess a wide range of skills, resources, and motivation ranging from the inquisitive browser with limited technical knowledge to those who are aware of the value of the information stored on the system, are prepared to devote significant resources in order to gain entry, and have some technical awareness of the system design.

36 It is assumed that the value of the stored assets does not merit stringent IT security controls. It is also assumed that the physical controls would alert the system authorities to the physical presence of attackers within the controlled space.

T.AUTHOR A user may gain access to resources for which no access rights have been granted.

37 The term user is used to cover persons who are granted some form of legitimate access to the system, but not necessarily to all data objects.

38 It is assumed that such persons may possess a wide range of technical skills and, because they have some rights of access, are minimally trusted not to attempt to subvert the system or exploit the information stored thereon. Some users may be motivated by curiosity to gain access to information for which they have no authority.

39 Two broad categories of users are identified with respect to this threat. The first category can be assumed to have limited technical skills and only be accessing the system through application level facilities. The second category can be assumed to be granted access to programming facilities with the appropriate technical skills and may attempt to bypass system controls as a technical challenge.

T.FLAW Security failures may occur because of flaws in the TOE.

40 The security of the TOE can be assured only if it has the right security features to counter the threats and the implementation of those features can be trusted to operate correctly.

41 Users or external threat agents may, through accidental discovery or directed search, discover flaws in the TOE construction or operation which result in exploitable vulnerabilities.

T.TRACE Security relevant events may not be recorded or may not be traceable to the user associated with the event.

42 Proper management and monitoring of the TOE security depends on the ability of the TOE to detect and report the occurrence of security relevant events, to

determine the identity of those responsible for such events, and to protect the event records from unauthorised access, modification, or destruction.

2.3.2.2 Threats to be addressed by the operating environment

43 The threat possibilities discussed below must be countered in order to support the CS1 security capabilities but are not addressed directly by CS1 compliant TOEs. Such threats must be addressed by the operating environment

T.OPERATE Security failures may occur because of improper administration and operation of the TOE.

44 The security offered by CS1 can be assured only to the extent that the TOE is operated correctly by system administrators and authorised users.

45 Users or external threat agents may, through accidental discovery or directed search, discover inadequacies in the security administration of the TOE which permit them to gain logical access to its resources in breach of any permissions they may have.

46 Potential attackers may seek to develop methods whereby the improperly administered security functions of the TOE may be circumvented during normal operation.

T.PHYSICAL Security-critical parts of the TOE may be subjected to physical attack which may compromise security.

47 The security offered by CS1 can be assured only against attacks on the TOE which seek to exploit its legitimate interfaces. It is therefore assumed that adequate physical controls are in place to prevent potential attack agents from gaining access to the TOE or the platform upon which the TOE is operating.

2.3.3 Organisational security policies

48 Within government environments, CS1 compliant TOEs are considered to be suitable to protect sensitive-but-unclassified or single level classified information.

49 For commercial environments, CS1 compliant TOEs are considered to be suitable to protect information in situations in which availability of that information needs to be restricted such that only designated users may access the information.

50 CS1 compliant products are not intended to protect multi-level classified information as they are not designed to enforce controls on the flow of information between objects at differing levels of information sensitivity.

51 The organisational security policies discussed below are addressed by CS1 compliant TOEs:

P.KNOWN Legitimate users of the TOE must be identified before TOE access can be granted.

52 CS1 assumes that there is a finite community of known users who will be granted rights of access and that system management has authority over that user community.

P.TRUST Legitimate users of the system, once granted access to information, are trusted to manage the subsequent control of that information.

53 CS1 is intended to satisfy the class of organisational security policies generally described as 'need-to-know'. Such policies place controls on the persons who are permitted access to specific objects such as files or documents.

54 Once granted legitimate access to information, users are expected to make further use of that information only in accordance with the organisational security policy. No mandatory controls are applied by the TOE.

P.ACCESS Access rights to specific data objects are determined by attributes assigned to that object, the identity of the user, and attributes associated with that user.

55 CS1 supports organisational policies which grant or deny access to objects using rules which are driven by attributes of the user (such as identity, affiliations etc.) and attributes of the object (such as owner, users allowed/denied access, affiliations allowed/denied access).

56 CS1 does not define the rules fully, rather it lays down the basic access control requirements and defers decisions on some of the detail to the Security Target.

P.ACCOUNT Users must be held accountable for their important security actions.

57 CS1 supports organisational policies which require that users can subsequently be held accountable for their actions.

58 Such policies permit investigations of security incidents which relate to incautious exercise of user discretion.

2.3.4 Secure usage assumptions

59 A CS1 conformant TOE is assured to provide effective security measures only if it is installed, managed, and used correctly. The operational environment must be managed according to the CS1 assurance requirements documentation for delivery, operation, and user and administrator guidance.

60 The following specific conditions are assumed to exist in a CS1 environment:

2.3.4.1 Physical assumptions

61 CS1 is intended for application in user areas that have physical control and monitoring. It is assumed that the following physical conditions will exist:

A.LOCATE The processing resources of the product, including terminals, will be located within controlled access facilities which will prevent unauthorised physical access.

A.PROTECT The TOE hardware and software critical to security policy enforcement will be physically protected from unauthorised modification by potentially hostile outsiders.

2.3.4.2 Personnel assumptions

62 It is assumed that the following personnel conditions will exist:

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.ACCESS Users possess the necessary privileges to access the information managed by the TOE.

A.COOP Users need to accomplish some task or group of tasks which requires a secure IT environment.

2.3.4.3 Connectivity assumptions

63 CS1 contains no explicit network or distributed system requirements. However, it is assumed that the following connectivity conditions exist:

A.PEER Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints.

64 CS1 is applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security requirements which address the need to trust external systems or the communications links to such systems.

A.CONNECT All connections to peripheral devices reside within the controlled access facilities.

65 CS1 only addresses security concerns related to the manipulation of the TOE through its legitimate interfaces. Internal communication paths to interface points such as terminals are assumed to be adequately protected.

2.4 Security objectives

2.4.1 IT security objectives

66 The following are the CS1 TOE IT security objectives:

- O.LOGICAL** The TOE must prevent logical entry to the TOE by persons with no authority to access the TOE.
- O.ACCESS** The TOE must limit user access to TOE resources to only those to which they have been granted access.
- O.RECORD** The TOE must record necessary events to ensure that the information exists to support effective security management.
- O.ACCOUNT** The TOE must ensure that all TOE users can subsequently be held accountable for their security relevant actions.
- O.BYPASS** The TOE must prevent illicit or errant software or users from bypassing TOE security policy enforcement.
- O.FLAW** The TOE must not contain obvious flaws in design, implementation, or operation.
- O.CONTROL** The TOE must provide all the functions and facilities necessary to support those responsible for the management of TOE security.

2.4.2 Non-IT security objectives

67 The CS1 TOE is assumed to be complete and self-contained and, as such, is not dependent upon any other products to perform properly. However, certain objectives with respect to the general operating environment must be met in order to support the CS1 security capabilities.

68 The following are the CS1 non-IT security objectives:

- O.INSTALL** Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.
- O.PHYSICAL** Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security.
- O.CREDEN** Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which maintains IT security.
- O.CONN** Those responsible for the TOE must ensure that no connections to outside systems or users can undermine the IT security objectives.

2.5 TOE IT security requirements

69 This section contains functional and assurance requirements that must be satisfied by a CS1 compliant TOE. These requirements consist of functional components

from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3.

2.5.1 Functional requirements

70 Table 2.1 below summarises the CS1 functional requirements as expressed in CC part 2 components:

	Component	Name	Refined
1	FIA_UID.1	User Identification	
2	FIA_UAU.1	Basic User Authentication	
3	FIA_ATD.1	User Attribute Definition	
4	FIA_ATA.1	User Attribute Administration	
5	FIA_ADP.2	Extended User Authentication Data Protection	
6	FAU_GEN.1	Audit Data Generation	Yes
7	FAU_GEN.2	User Identity Generation	
8	FAU_STG.1	Security Event Storage	
9	FAU_PRO.1	Security Audit Trail Protection	
10	FAU_MGT.1	Audit Trail Management	Yes
11	FAU_SEL.1	Selective Audit	Yes
12	FAU_SEL.2	Runtime Selection Mode	
13	FPT_TSA.1	Basic Security Administration	
14	FPT_TSU.1	Administrative Safe Use	
15	FDP_ACC.1	Subset Object Access Control	Yes
16	FDP_ACF.1	Single Security Attribute Access Control	Yes
17	FDP_ACI.1	Static Attribute Initialisation	
18	FDP_SAM.2	Security Attribute Modification	Yes
19	FDP_RIP.1	Subset Residual Information Protection	Yes
20	FPT_SEP.1	TSF Domain Separation	Yes
21	FPT_RVM.1	Non-Bypassability of TSP	Yes
22	FPT_AMT.1	Abstract Machine Testing	Yes

Table 2.1 - Functional components of CC/CS1

2.5.1.1 Identification and authentication requirements

71 **FIA_UID.1.1** The TSF shall identify each user before performing any actions requested by the user.

72 **FIA_UAU.1.1** The TSF shall authenticate any user's claimed identity prior to performing any functions for the user.

73 **FIA_ATD.1.1** The TSF shall provide, for each user, a set of security attributes necessary to enforce the TSP.

74 **FIA_ATA.1.1** The TSF shall provide the ability to initialise user attributes with provided default values.

75 **FIA_ADP.2.1** The TSF shall protect from unauthorised observation, modification, and destruction the raw form of authentication data at all times while it resides in the TOE.

2.5.1.2 **Audit requirements**

76 **FAU_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:

- a) Startup and shutdown of the audit functions.
- b) All auditable events for the basic level of audit, as defined in all functional components included in CC/CS1:
 - 1) [FIA_UID] All attempts to use the user identification mechanism, including the user identity provided. The origin of request shall be included in the audit record.
 - 2) [FIA_UAU] Any use of the authentication mechanism. The origin of request shall be included in the audit record.
 - 3) [FIA_ATA] All attempted uses of the user attribute administration function including Identification of the user attributes that have been modified.
 - 4) [FIA_ADP] All requests to access user authentication data.
 - 5) [FAU_PRO] Any attempt to read, modify, or destroy the audit trail.
 - 6) [FAU_MGT.1] Any attempt to perform an operation on the audit trail.
 - 7) [FAU_SEL] All modifications to the audit configuration that occur while the audit collection functions are operating.
 - 8) [FDP_ACF] All requests to perform an operation on an object covered by the Discretionary Access Control Policy including introduction of objects into a user's address space, and deletion of objects.
 - 9) [FDP_ACI] Any changes or overriding of the default object attributes including which default object attributes have been changed or overridden.
 - 10) [FDP_SAM] All attempts to modify security attributes including the identity of the target of the modification attempt and the new values of the modified security attributes
 - 11) [FPT_AMT] Execution of the tests of the underlying machine and the results of the tests.
 - 12) [FPT_TSA] Use of a security relevant administrative function.

c) [assignment: *other auditable events*]

77 **FAU_GEN.1.2** The TSF shall record within each audit record at least the following information:

- a) date and time of event, type of event, subject identity, and outcome (i.e. success or failure) of the event.
- b) For each audit record type, based on the auditable event definitions of the functional components included in CC/CS1, [assignment: *other information relevant to the audited event*].

78 **FAU_GEN.2.1** The TSF shall be able to associate any auditable events with the identity of the user responsible for the events.

79 **FAU_STG.1.1** The TSF shall store generated audit records in a permanent audit trail.

80 **FAU_PRO.1.1** The TSF shall restrict access to the audit trail to the authorised administrator.

81 **FAU_MGT.1.1** The TSF shall provide the authorised administrator with the ability to create, delete, and empty the audit trail.

82 **FAU_SEL.1.1** The TSF shall be able to include or exclude auditable events from the set of audited events based on one or more of the following attributes:

- a) User identity
- b) Object attributes

83 **FAU_SEL.2.1** The TSF shall provide the authorised administrator with the capability to select, at any time during the operation of the TOE, which events are to be audited.

2.5.1.3 TOE administration requirements

84 **FPT_TSA.1.1** The TSF shall distinguish security-relevant administrative functions from other functions.

85 **FPT_TSA.1.2** The TSF's set of security-relevant administrative functions shall include all functions necessary to install, configure, and manage the TSF; minimally, this set shall include:[assignment: list of administrative services to be minimally supplied]

86 **FPT_TSA.1.3** The TSF shall restrict the ability to perform security-relevant administrative functions to specifically authorised users.

87 **FPT_TSA.1.4** The TSF shall be capable of distinguishing the set of users authorised for administrative functions from the set of all users of the TOE.

88 **FPT_TSU.1.1** The TSF shall enforce checks for valid input values for security relevant administrative functions as described in the Administrative Guidance.

2.5.1.4 Access control requirements

89 **FDP_ACC.1.1** The TOE shall enforce the Discretionary Access Control Policy on:

- a) users
- b) subjects acting upon behalf of users
- c) other named subjects
- d) named objects which contain user data
- e) [assignment: *operations among subject and objects covered by the access rules*].

90 **FDP_ACF.1.1** The TSF shall enforce the Discretionary Access Control Policy on objects based on the following subject attributes:

- a) user identity: user identity from user attributes
- b) group list: zero or more group identities from user attributes
- c) [assignment: *subject type: nature of the subject*]

91 **FDP_ACF.1.1** The TSF shall enforce the Discretionary Access Control Policy on objects based on the following object attributes:

- a) access control list: a list of groups and users with, for each group or user, a list of the specific operations permitted on the object by each group or user;
- b) [assignment: *object type: the nature of the controlled object*].

92 **FDP_ACF.1.2** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- a) If the subject user identity or any member of the subject group list is mentioned in the access control list of the object, then the subject shall be granted the access permissions mentioned in the access control list.
- b) If neither the subject user identity nor any member of the subject group list is mentioned in the access control list of the object, then access shall be granted by application of the [assignment: *default access rules*].
- c) If consulting the access control list returns a non-unique result, then the ambiguity shall be resolved by application of [assignment: *rules for the consultation of access control lists*].

93 If different rules apply to different subjects and objects, the totality of these rules shall be shown to support the overall policy.

94 **FDP_ACI.1.1** The TSF shall enforce the Default Attributes Policy to provide valid user supplied or default values for the object security attributes that are used to enforce the policy.

95 **FDP_ACI.1.2** The TSF shall allow the specification of alternate initial values to override the default values when the object is created.

96 **FDP_SAM.2.1** The TSF shall enforce the following access rules to provide authorised users with the ability to modify object attributes.

a) Access permission to an object by users not already possessing access permission shall be assigned only by authorised users.

b) [assignment: *additional rules for the modification of object attributes*]

These rules shall allow authorised users to specify and control sharing of objects by named individuals or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights.

If different rules of assignment and modification of access control attributes apply to different subjects and/or objects, the totality of these rules shall be shown to support the defined policy.

97 **FDP_RIP.1.1** The TSF shall ensure that upon the allocation of a resource to objects which contain user data any previous information content (including encrypted representations) is unavailable.

2.5.1.5 Protection of TSF and reference mediation

98 **FPT_SEP.1.1** The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

a) The transfers between TSF and non-TSF domains shall be controlled such that arbitrary entry to or return from the TSF is not possible.

b) User or application parameters passed to the TSF by reference shall be validated with respect to the TSF address space, and those passed by value shall be validated with respect to the values expected by the TSF.

c) The permissions of objects (and/or to non-TSF data) passed as parameters to the TSF shall be validated with respect to the permissions required by the TSF.

d) References to TSF objects used by TSF isolation functions shall be mediated by the TSF.

e) The TSF domain shall include all user and object attributes.

99 **FPT_SEP.1.2** The TSF shall enforce separation between the security domains of subjects in the TSC.

100 **FPT_RVM.1.1** The TSF shall ensure that the TSP enforcement functions are invoked and succeed before any security related operation is allowed to proceed.

a) The TSF shall mediate all references to subjects, objects, resources, and TSF functions.

- b) The mediation shall ensure that all subject object references are directed to the Discretionary Access Control Policy functions.
- c) The mediation shall ensure that all resource references are directed to the residual information protection functions.
- d) References issued by privileged subjects shall be mediated in accordance with the policy attributes defined for those subjects.

101 **FPT.AMT.1.1** The TSF shall provide the authorised administrator with the capability to validate the correct operation of the security-relevant functions provided by the hardware and firmware upon which the TOE operates.

2.5.2 Assurance requirements

102 The TOE shall meet the requirements of Evaluation Assurance Level EAL3 with respect to the functional requirements.

2.6 Environmental IT security requirements

103 CS1 is primarily applicable to TOEs which are fully responsible for enforcement of the TOE Security Policy (TSP) and do not, therefore, require that the IT environment of the TOE accept any TSP enforcement responsibility.

104 Application of CS1 to a TOE which requires some of the CS1 IT security requirements to be met by the TOE IT environment is permissible. Should this be the case, the Security Target must explain the partition of security requirements between the TOE and its IT environment and demonstrate that the TOE in its IT environment satisfies all of the CS1 security requirements.

2.7 Application notes

105 This section is used to provide additional information which will be of value to the ST writer when interpreting the CC requirements for inclusion in the ST. This additional information consists of background refinement information and notes specific to each operation that has not been completed in the PP.

- a) **FIA_UID.1.1** note that CC/CS1 does not enforce uniqueness of user ids. It meets the requirement 'shall be able to enforce individual accountability' only if the administration does not define duplicate user identities.
- b) **FIA_UAU.1.1**
No specific authentication mechanisms are identified in the PP, suitable mechanisms would include passwords and token based controls.
- c) **FIA_ATD.1.1**
The PP enforces does not enforce unique user id requirements, management will have to ensure this if it is required.

- d) **FIA_ADP.2.1**
This calls for positive measures to protect the authentication mechanism. Examples are encryption of the password file to cover accidental disclosure, and overwriting passwords as they are entered on the screen. This requirement is not intended to address password management issues such as ageing.
- e) **FAU_GEN.1.1**
This element identifies possible audit records to the extent that is possible at the level of requirements expression. The ST author must tailor these in line with the specific TOE characteristics and the characteristics of the event audited. Operations are left open to permit the ST author to add further requirements to audit administrative actions and any other events that are held to be significant.
- f) **FAU_GEN.1.2**
This element identifies the contents of the audit record and must include the information necessary (e.g. terminal id) to trace back to the event originator and the action invoked. An operation is left open to add further information to the ST.
- g) **FAU_MGT.1.1**
Audit management facilities are minimal in this profile. ST writers should consider extending the scope of the ST to include some CC audit trail display and processing components.
- h) **FAU_SEL.1.1**
The audit event selection options must be based on the information listed but the particular selection rules which are implemented must be defined and explained in the ST. These should permit the authorised administrator to balance the security needs with the volume of audit data generated and the resource demands of the audit function.
- i) **FPT_TSA.1.2**
The specific administrative services offered are left as an operation which the ST author must complete. The extent and utility of such services is dependent on the nature and scale of the TOE. The evaluator will consider whether the services, or lack of provision of services, leads to insufficient security of the TOE. FC/CS1 does not identify particular configuration and administration functions. ST writers should consider using FPT_TSM framework to define them.
- j) **FDP_ACC.1.1**
CC/CS1 is intended to apply to a range of discretionary policies and thus cannot be specific about the policy details. The DAC model of user object mediation is mandated but the ST writer must identify the following in the appropriate operations or refinements:
 - 1) Other subjects (if any) apart from users and their proxies, e.g. system processes and servers.

- 2) The controlled objects, e.g. files, database domains, shared memory regions, or peripheral devices.
 - 3) Subject/object operations which are to be controlled such as read, write, delete, execute, or change attributes.
- k) **FDP_ACF.1.1 - subject attributes**
CC/CS1 is not specific about policy details and permits decisions to be based on subject attributes defined in the ST. As a minimum, the concept of users and groups must be supported. The operation allows other subject attributes to be identified such as user or system process.
- l) **FDP_ACF.1.1 - object attributes**
CC/CS1 is not specific about policy details above a required minimum. The operation permits the ST author to define object attributes over and above the access control list, and default permissions. Examples might be to use different rule sets for executable files from data access rules.
- m) **FDP_ACF.1.2**
This requirement permits the ST author to express the detailed access control rules. The minimum of access control list resolution is mandatory. The details of the rules for resolution of no reference within, or conflict within the access control list must be supplied by the ST author in the operation. Permissive or restrictive resolution are options and the details are TOE specific. If necessary, different rule sets may be defined for different subject types subject to a consistent overall policy.
- n) **FDP_SAM.2.1**
The details of the object attribute modification policy are not addressed in the PP and must be completed by the ST author. ST authors should check that the policy details meet the organisational policy objectives of the TOE whilst not being overly restrictive and intrusive in use. Some interpretation of the original FC/CS1 requirements is necessary here.

Chapter 3

Commercial Security 3 (CS3) Protection Profile

NOTE TO READER: This version 1.0 of the CS3 Protection Profile (PP) is still rather incomplete. Due to production deadlines for other parts of the CC version 1.0 upon which this PP depends, insufficient time was available to fulfil the goal of full modelling of the CS3 set of requirements contained in the Federal Criteria. While it is believed that the functional requirement components selected here are the appropriate set for CS3, at the time of publication no rigorous cross-check could be made of them against the Federal Criteria. In particular, a large number of the ‘operations’ on the selected functional requirements remain incomplete and therefore do not reflect all of the requirement details contained in the Federal Criteria. It is anticipated that the next version of this PP will fully meet the intended goal.

3.1 Introduction

3.1.1 Identification

106 Title: Commercial Security 3 (CS3) - Role-Based Access Protection.

107 Registration: <to be filled in by registry>

108 Keywords: Access control, role-based access, non-discretionary controls, general-purpose operating system, information protection.

3.1.2 Protection Profile overview

109 CS3 uses the CC requirements components to model the CS3 profile from the Federal Criteria (FC). CS3 specifies a strong set of security functions and assurances for general purpose multi-user operating systems, database management systems, and other applications in sensitive environments. CS3 is intended for environments in which access to programs, transactions, and information must be restricted according to the assigned organisational role(s) of users.

110 CS3 supports a variety of organisation specific non-discretionary integrity and confidentiality policies calling for role-based access controls. CS3 provides strong authentication mechanisms and administrative tools.

111 CS3 compliant products are expected to be used in sensitive commercial and governmental environments where system failure is not tolerated and a relatively high degree of confidence is required. For governmental environments, CS3 compliant products are intended to process sensitive unclassified or single-level classified but not multi-level classified information.

3.2 TOE description

- 112 CS3 defines a set of security requirements to be levied on Targets of Evaluation (TOEs) which include general purpose operating systems, database management systems, and other applications.
- 113 Such TOEs implement the basic services which permit IT applications to access and manage the computing hardware resources and interact with users and other applications in a controlled and protected manner. CS3 compliant TOEs permit multiple users to perform a variety of functions based on defined roles, which allow controlled shared access to data and IT processes.
- 114 CS3 TOEs are resistant to resource depletion and system failure by providing a variety of system recovery and resource allocation features.
- 115 Typical CS3 installations are workgroup or enterprise computing systems with strong need-to-know and data integrity requirements, accessed by users local to, or with otherwise protected access to, the computer systems.
- 116 CS3 is applicable to TOEs that provide facilities for on-line interaction with users. CS3 is also generally applicable to TOEs incorporating network functions but contains no network specific requirements. Networking is covered only to the extent to which it can be considered part of a centrally-managed system that meets a common set of security requirements.
- 117 CS3 assumes that the organisation is the owner of all data. All data is centrally administered and is under the control of the operating system. The data is stored in named objects, and the operating system can associate with each object a finely-grained description of the access rights to that object.
- 118 All individual users are assigned a unique user identifier. This user identifier supports individual accountability. The TOE authenticates the claimed identity of the user before allowing the user to perform any further actions. CS3 supports multiple authentication mechanisms.
- 119 A CS3 compliant TOE enforces controls such that access to the data objects and permitted actions with respect to them can only take place in accordance with the role-based access restrictions placed on that object by the system administrator. The system administrator will associate each user with one or more roles which the TOE will use to make access decisions. Authority to assume a role can only be granted and revoked by the system administrator. A set of operations is allocated to each role by the system administrator. Each operation includes an action or transformation procedure and a set of associated data items. A role is a set of non-discretionary associations of user - operations - data objects.
- 120 CS3 supports the policy of separation of duties, in which roles may not conflict. No single individual would be authorised to perform all parts of a transaction represented by a set of operations against a set of data objects. This capability can be extended to system administrators in order to prevent a 'privileged user' or 'superuser' from having a wide set of privileges when only a subset is needed.

- 121 A CS3 compliant TOE is assured to provide effective security measures only if it is installed, managed, and used correctly. The operational environment must be managed in a manner that supports the CS3 security objectives. In particular this includes allowing a determination that the evaluated TOE has been received without modification, that a secure state has been established during installation, and that the secure state is maintained during operation.

3.3 Security environment

3.3.1 Summary

- 122 This section identifies the security issues which form the basis for choice of the CS3 security requirements. It identifies assumptions about the physical, personnel and other aspects of the environment of the TOE, the organisational security policies for which CS3 compliant TOEs are appropriate, and the threats to the data security which the CS3 requirements are intended to counter.

3.3.2 Secure usage assumptions

- 123 A CS3 compliant TOE is assured to provide effective security measures only if it is installed, managed, and used correctly. The operational environment must be managed according to the CS3 assurance requirements documentation for delivery, operation, and user and administrator guidance.

- 124 The following specific conditions are assumed to exist in a CS3 environment:

3.3.2.1 Physical assumptions

- 125 CS3 is intended for use in areas that have differing levels of physical control and monitoring. It is assumed that the following physical conditions will exist:

A.LOCATE Some, but not necessarily all, processing resources of the TOE, including terminals, will be located within controlled access facilities which will prevent unauthorised physical access.

A.PROTECT The TOE hardware and software critical to security policy enforcement will be physically protected from unauthorised modification by potentially hostile outsiders.

3.3.2.2 Personnel assumptions

- 126 It is assumed that the following personnel conditions will exist:

A.MANAGE There will be one or more competent individuals assigned to manage the TOE, including the security of the information it contains and the allocation of levels of system resources.

A.ACCESS Users possess the necessary privileges, based on roles, to access the information managed by the TOE.

A.COOP Users need to accomplish some task or group of tasks which requires an IT environment supportive of the tasks whilst providing the necessary security controls.

3.3.2.3 Connectivity assumptions

127 CS3 contains no explicit network or distributed system requirements. However, the specification of resource access control is sufficiently flexible for a developer to define a policy for dealing with networks at the CS3 level.

128 It is assumed that the following connectivity conditions exist:

A.PEER Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints.

129 CS3 is applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security requirements which address the need to trust external systems or the communications links to such systems.

A.CONNECT All connections to peripheral devices reside within the controlled access facilities.

130 CS3 only addresses security concerns related to the manipulation of the TOE through its legitimate interfaces. Internal communication paths to interfaces points such as terminals are assumed to be adequately protected.

3.3.3 Organisational security policies

131 CS3 is capable of enforcing a broad class of organisational security policies which include:

- specification of user capability to perform specific tasks;
- enforcement of least privilege for administrators and users; and
- specification and enforcement of conflicts-of-interest rules which may entail duty assignment and separation of duties.

132 For commercial environments, CS3 compliant TOEs are considered to be suitable to protect information in situations in which access to and operations on that information need to be closely controlled.

133 For government environments, CS3 compliant TOEs are considered to be suitable to protect sensitive-but-unclassified or single level classified information. CS3 compliant TOEs are not intended to protect multi-level classified information, as

they are not specifically designed to control the flow of information between higher and lower levels of information sensitivity.

134 The organisational security policies discussed below are addressed by CS3 compliant TOEs.

P.OWNER The organisation is the 'owner' of information and controls all access to it.

135 CS3 assumes that legitimate users of the system, once granted access to a data object, may not be trusted to manage the subsequent control of that data themselves.

P.KNOWN Legitimate users of the system must be identified before rights of access can be granted.

136 CS3 assumes that there is a finite community of known users who will be granted rights of access and that system management has authority over that user community.

P.ROLE Rights for users to gain access to and perform operations on information must be based on identity-based 'need-to-know' and assigned role with respect to the information.

137 CS3's ability to enforce user access to data objects makes it equally applicable to the class of organisational security policies generally described as 'need-to-know'.

P.DUTY Important information must be protected by 'separation of duties', such that no single user may be granted the right to perform all operations on it.

138 CS3 is capable of enforcing separation of duties through its role-based ability to restrict users to specific data objects and to specific actions upon those objects.

P.ACCOUNT Users must be held accountable for the security relevant actions they perform.

139 CS3 supports organisational security policies which require that users can subsequently be held accountable for their actions.

140 Such policies permit investigations of security incidents which relate to incautious exercise of user discretion.

3.3.4 Threats to security

141 CS3 compliant TOEs are required to counter threats which may be broadly categorised as the threat of attack from hostile outsiders with no legitimate access to the system, and threats from insiders with legitimate access to the system attempting to gain access to and perform operations on information for which they have no individually defined rights. In addition, certain threats of a non-IT nature can affect the security of CS3 compliant TOEs and must be dealt with by the operating environment.

3.3.4.1 Threats addressed by TOE

142 The threat possibilities discussed below are addressed by CS3 compliant TOEs.

T.ACCESS An unauthorised person may gain logical access to the TOE.

143 The term unauthorised person is used to cover all those persons who have, or may attempt to gain, physical access to the system and its terminals but have no authority to gain logical access to the system or perform operations on its information.

144 It is assumed that such unauthorised persons could possess a wide range of skills, resources, and motivation ranging from the inquisitive browser with limited technical knowledge to those who are aware of the value of the information stored on the system, are prepared to devote significant resources in order to gain entry, and have some technical awareness of the system design.

145 It is also assumed that the value of the stored assets merits moderately intensive penetration or masquerading attacks. It is also assumed that physical controls in place would alert the system authorities to the physical presence of attackers within the controlled space.

T.AUTHOR A user may gain access to resources or perform operations for which no access rights have been granted.

146 The term user is used to cover those who are granted some form of legitimate access to the system, but not necessarily to all data objects or possible operations on those objects.

147 It is assumed that such persons may possess a wide range of technical skills and, because they have some rights of access, are minimally trusted not to attempt to subvert the system or exploit the information stored thereon. However, in view of the need for separation of function inherent in the selection of CS3, it is assumed that there is some potential for personal gain to users from attempts to perform operations on data for which they have no authority. Some users may also be motivated by curiosity to gain access to information for which they have no authority.

148 Two broad categories of users are identified with respect to this threat. The first category can be assumed to have limited technical skills and only be accessing the system through application level facilities. The second category can be assumed to be granted access to programming facilities with the appropriate technical skills and may attempt to bypass system controls as a technical challenge.

T.TRACE Security relevant events may not be recorded or may not be traceable to the user associated with the event.

149 Proper management and monitoring of the TOE security depends on the ability to detect and report the occurrence of security relevant events, to determine the identity of those responsible for such events, and to protect the records of such

events from unauthorised access, modification, or destruction. Close personal accountability of user actions and quick reporting of anomalous system events is critical to the CS3 approach.

- 150 It may not be possible to detect an attack on the TOE because the audit records may not cover security significant events or may not be available. Also, it may not be possible to correctly attribute recorded events to users. Either condition leads to a risk that it may not be possible to respond appropriately to attacks on the system.

T.FLAW Security failures may occur because of flaws in the TOE.

- 151 The security offered by CS3 can be assured only to the extent that all of the security features of the TOE can be trusted to be effective in countering the threats and to operate correctly and reliably.

- 152 Users or external threat agents may, through accidental discovery or directed search, discover flaws in the TOE which may be subverted such that the operation of the security functions is changed to their advantage.

- 153 Such subversion of the TOE may occur during delivery and installation. During normal operation, potential attackers may also seek to develop methods whereby the TOE's integrity, and hence its security functions, may be undermined.

T.DENY Users may be denied accessibility to the resources of the TOE.

- 154 CS3 is intended for use in organisations that are intolerant of the non-availability of system resources. Degradation of system resource availability can occur from a variety of causes related to intentional and unintentional occurrences.

- 155 System resource management, users, and external threat agents can all cause degradation or non-availability of resources, especially disk space, memory, and CPU usage.

T.CRASH The secure state of the TOE could be compromised in the event of a system crash.

- 156 For the CS3 TOE to protect the information it controls, it must remain in a secure state at all times during operation. That secure system state must be recovered in the event of a system failure or discontinuity of service.

- 157 System crash can occur with inadequate mechanisms for recovery on system start-up. User data objects and audit information may be modified or lost in the event of a system crash from any of a variety of causes. System and application software may also be harmed under such conditions.

T.TAMPER Protection relevant mechanisms of the TOE could be tampered with.

- 158 The TOE's software and data that are involved with the enforcement of TOE security could be bypassed or compromised, reducing the integrity of the enforcement mechanisms and disabling their ability to manage the TOE security.

T.OBSERVE Events may occur in TOE operation that compromise IT security but which may not be readily noticed.

159 This threat addresses the human factor relating to the ability of the administrator or user to detect a problem that occurs affecting the TOE's security state. The TOE could subsequently be used in a manner which is insecure but which the administrator or user might reasonably but incorrectly believe to be secure. The un-noticed security problem itself could arise from a number of different factors. For example, it may be possible that human or other errors in operation could deactivate or disable TOE security functions, the TOE may crash and return to operation in an insecure state, or the TOE could also be installed or configured in a way which is insecure.

3.3.4.2 Threats to be addressed by the operating environment

160 The threat possibilities discussed below must be countered in order to support the CS3 security capabilities but are not addressed by CS3 compliant TOEs. Such threats must be addressed by the operating environment.

T.INSTALL The TOE may be delivered and installed in a manner which undermines security.

161 The security offered by CS3 is predicated upon the TOE being initially established in a secure state. That includes assurance that the TOE delivered is that which was evaluated and that the TOE is subsequently installed properly.

T.PHYSICAL The TOE may be subjected to physical attack which may compromise security.

162 The security offered by CS3 can be assured only if the TOE is protected from direct physical attack. It is therefore assumed that adequate physical controls are in place to prevent potential attack agents from gaining access to the TOE or the platform upon which the TOE is operating. Note that this threat is more general than T.TAMPER, which relates to a physical attack directed against

T.OPERATE Security failures may occur because of improper administration and operation of the TOE.

163 The security offered by CS3 can be assured only to the extent that the TOE is operated correctly by system administrators and users.

164 Users or external threat agents may, through accidental discovery or directed search, discover inadequacies in the security administration of the TOE which permit them to gain logical access to and perform operations on its resources in breach of any permissions they may have.

165 Potential attackers may seek to develop methods whereby the improperly administered security functions of the TOE may be circumvented during normal operation.

T.ROLEDEV The development and assignment of user roles may be done in a manner which undermines security.

166 In general, roles could be developed which have an incorrect or improper combination of authorisations to perform operations on objects. Also, users could be assigned to roles that are incommensurate with their duties, giving them either too much or too little scope of authorisation.

167 A particular concern arises in that users could be assigned conflicting roles with respect to 'separation of duties'. An individual user could be authorised to perform multiple operations on data objects that represent the parts of a transaction which should be separated among different individuals.

3.4 Security objectives

3.4.1 IT security objectives

168 The following are the CS3 TOE IT security objectives:

O.LOGICAL The TOE must strongly prevent logical entry to it by persons or processes with no rights to access it.

O.LOCATE The TOE must be able to restrict user entry to it based on time and entry device location.

O.ROLE The TOE must prevent users from gaining access to and performing operations on its resources for which their role does not have explicit permission.

O.RECORD The TOE must record necessary events to ensure that the information exists to support effective security management.

O.ACCOUNT The TOE must ensure that all users can be held accountable for their security relevant actions.

O.TAMPER The TOE must prevent physical tampering with its security-critical parts.

O.BYPASS The TOE must prevent illicit or errant software or users from bypassing TOE security policy enforcement.

O.FLAW The TOE must not contain flaws in design, implementation, or operation.

O.CONTROL The TOE must provide all the functions and facilities necessary to support those responsible for the management of TOE security.

O.OPERATE The TOE must ensure the continued correct operation of its security functions.

O.ACCESS The TOE must ensure the continued accessibility of TOE resources by authorised users.

O.OBSERVE The TOE must ensure that its security status is readily observable and controllable by the system administrator at all times.

O.PRESERV The TOE must ensure that its secure state is preserved in the event of a system failure or discontinuity of service.

3.4.2 Non-IT security objectives

169 The CS3 TOE is assumed to be complete and self-contained and, as such, is not dependent upon any other products to perform properly. However, certain objectives with respect to the general operating environment must be met in order to support the CS3 security capabilities.

170 The following are the CS3 non-IT security objectives:

O.INSTALL Those responsible for the TOE must ensure that it is delivered and installed in a manner which maintains IT security.

O.MANAGE Those responsible for the TOE must ensure that it is managed, administered and operated in a manner which maintains IT security.

O.PHYSICAL Those responsible for the TOE must ensure that the TOE is protected from physical attack which might compromise IT security.

O.ROLEDEV Those responsible for the TOE must ensure that the development and assignment of roles is done in a manner which maintains IT security.

O.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which maintains IT security.

O.CONNECT Those responsible for the TOE must ensure that no connections to outside systems or users undermine the IT security.

3.5 TOE IT security requirements

171 This section contains functional and assurance requirements that must be satisfied by a CS3 compliant TOE. These requirements consist of functional components from Part 2 of the CC and an augmented Evaluation Assurance Level (EAL) containing assurance components from Part 3.

3.5.1 Functional requirements

172 Table 3.1 below summarises the CS3 functional requirements as expressed in CC Part 2 components. Following the table, details of each required functional

component are provided, including the elements and the operations performed on them to meet specific needs of CS3.

Component	Name
FIA_ADA.3	Expanded User Authentication Data Administration
FIA_ADP.1	Basic User Authentication Data Protection
FIA_ADP.2	Extended User Authentication Data Protection
FIA_AFL.2	Administrator Controlled Authentication Failure Handling
FIA_ATA.1	User Attribute Initialisation
FIA_ATA.2	Basic User Attribute Administration
FIA_ATD.1	Shared User Attribute Definition
FIA_ATD.2	Unique User Attribute Definition
FIA_SOS.1	Selection of Secrets
FIA_SOS.2	TSF Generation of Secrets
FIA_UAU.1	Basic User Authentication
FIA_UAU.6	Configurable Authentication Mechanisms
FIA_UAU.9	Installable Authentication Mechanisms
FIA_UID.2	Unique identification of users
FIA_USB.1	User-Subject Binding
FTA_LSA.1	Limitation on Scope of Selectable Attributes
FTA_MCS.2	Per User Attribute Limitation on Multiple Concurrent Sessions
FTA_SSL.1 OR FTA_SSL.3	Session Locking and Unlocking OR TSF-initiated Termination
FTA_SSL.2	User-initiated Locking
FTA_TAB.2	Configurable TOE Access Banners
FTA_TAH.1	TOE Access History
FTA_TAM.1	Basic TOE Access Management
FTA_TSE.1	TOE Session Establishment
FTP_TRP.1	Trusted Path
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Single Security Attribute Access Control
FDP_ACF.3	Access Authorisation
FDP_ACF.4	Access Authorisation and Denial
FDP_ACI.3	Basic Attribute Initialisation
FDP_RIP.2	Full Residual Information Protection
FDP_SAM.2	Basic Attribute Modification
FDP_SAM.3	Safe Attribute Modification
FDP_SAQ.1	Administrator Attribute Query

Table 3.1 - CS3 functional requirements

Component	Name
FDP_SAQ.2	User Attribute Query
FAU_ARP.1	Security Alarms
FAU_ARP.2	Automatic Response
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	Individual Identity Generation
FAU_MGT.1	Audit Trail Management
FAU_MGT.3	Audit Trail Saturation Management
FAU_PAD.1	Profile Based Anomaly Detection
FAU_PIT.1	Simple Attack Heuristics
FAU_PRO.2	Extended Audit Trail Access
FAU_SAA.1	Imminent Violation Analysis
FAU_SAR.2	Extended Audit Review
FAU_SEL.1	Selective Audit
FAU_SEL.2	Runtime Selection Mode
FAU_SEL.3	Restricted Runtime Display Mode
FAU_STG.1	Permanent Audit Trail Storage
FAU_STG.3	Prevention of Audit Data Loss
FPT_AMT.3	Abstract Machine Test During Normal Operation
FPT_FLS.1	Failure with Preservation of Secure State
FPT_PHP.1	Passive Detection of Physical Attack
FPT_RCV.2	Automated Recovery
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SAE.1	Time-Limited Authorisation
FPT_SEP.1	TSF Domain Separation
FPT_SWM.1	Protection of Executables
FPT_TDC.1	Inter-TSF Basic TSF Consistency
FPT_TSA.2	Separate Security Administrative Roles
FPT_TSM.1	Management Functions
FPT_TST.3	TSF Testing During Normal Operation
FPT_TSU.1	Enforcement of Administrative Guidance
FRU_RSA.1	Maximum Quotas

Table 3.1 - CS3 functional requirements

3.5.1.1 Identification and authentication requirements

FIA_ADA.3 Expanded User Authentication Data Administration

173 FIA_ADA.3.1 The TSF shall provide functions for initialising and modifying user authentication data related to [assignment: *identified authentication mechanism*].

174 FIA_ADA.3.2 The TSF shall restrict use of these functions on the user authentication data for any user to the authorised administrator.

175 FIA_ADA.3.3 The TSF shall allow authorised users to use these functions to modify their own authentication data in accordance with the TSP.

176 Refinement:

- a) If passwords are used,
 - 1) The authorised user shall be allowed to modify his/her own authentication data within prescribed limits.
 - 2) The TSF shall provide a protected mechanism to allow a user to change his or her password. This mechanism shall require re-authentication of the user identity.

FIA_ADP.1 Basic User Authentication Data Protection

177 FIA_ADP.1.1 The TSF shall protect from unauthorised observation, modification and destruction authentication data that is stored in the TOE.

178 Refinement:

- a) The TSF shall store passwords in a one-way encrypted form.

FIA_ADP.2 Extended User Authentication Data Protection

179 FIA_ADP.2.1 The TSF shall protect from unauthorised observation, modification and destruction the raw form of authentication data at all times while it resides in the TOE.

180 Refinement:

- a) The TSF shall automatically suppress or fully blot out the clear-text representation of the password on the data entry/display device.

FIA_AFL.2 Administrator Controlled Authentication Failure Handling

181 FIA_AFL.2.1 The TSF shall be able to terminate the user session establishment process after [assignment: *number*] unsuccessful authentication attempts.

182 FIA_AFL.2.2 After the termination of a user session establishment process, the TSF shall provide the authorised administrator with the ability to specify whether the *user account* is to be disabled until [assignment: *conditions for re-enabling the user session establishment process*].

183 Refinement:

- a) The TSF shall appear to perform the entire user authentication procedure even if the user identification entered is invalid. Error feedback shall contain

no information regarding which part of the authentication information is incorrect.

- b) The TSF shall end the attempted login session if the user performs the authentication procedure incorrectly for a number of successive times (i.e., a threshold) specified by an authorised system administrator. The default threshold shall be three times. When the threshold is exceeded, the TSF shall delay the next login by an interval of time specified by the authorised system administrator. The default time interval shall be 60 seconds.

FIA_ATA1 Shared User Attribute Definitions

184 FIA_ATA.1.1 The TSF shall provide the ability to initialise user attributes with provided default values.

FIA_ATA.2 Basic User Attribute Administration

185 FIA_ATA.2.1 The TSF shall provide the ability to display and modify user attributes.

186 FIA_ATA.2.2 The TSF shall limit the ability to modify user attributes to only the authorised administrator.

FIA_ATD.1 Shared User Attribute Definition

187 FIA_ATD.1.1 The TSF shall provide, for each user, a set of security attributes necessary to enforce the TSP.

FIA_ATD.2 Unique User Attribute Definition

188 FIA_ATD.2.1 The TSF shall provide, for each user, a unique set of security attributes necessary to enforce the TSP.

NOTE: If the TOE provides the capability for user-generated passwords, then the following component FIA_SOS.1, Selection of Secrets, shall be selected. See section 3.7, Application notes.

FIA_SOS.1 Selection of Secrets

189 FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

190 Refinement:

- a) Passwords shall not be reusable by the same user identifier for a system-specifiable period of time. The default shall be six months.
- b) The TSF shall not indicate to the user if he/she has chosen a password already associated with another user.

- c) The TSF shall, by default, prohibit the use of null passwords during normal operation.
- d) The TSF shall provide an algorithm for ensuring the complexity of user-entered passwords that meets the following requirements:
 - 1) (1) Passwords shall meet a system-specifiable minimum length requirement. The default minimum length shall be eight characters.
 - 2) (2) The password complexity-checking algorithm shall be modifiable by the TSF. The default algorithm shall require passwords to include at least one alphabetic character, one numeric character, and one special character.
 - 3) (3) The TSF should provide a protected mechanism that allows systems to specify a list of excluded passwords (e.g., company acronyms, common surnames).
 - 4) (a) The TSF should prevent users from selecting a password that matches any of those on the list of excluded passwords.
- e) The control of password complexity shall be limited to system administrators.

NOTE: If the TOE provides the capability for TSF-generated passwords, then the following component FIA_SOS.2, TSF Generation of Secrets, shall be selected. See section 3.7, Application notes.

FIA_SOS.2 TSF Generation of Secrets

191 FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet [assignment: *a defined quality metric*].

192 FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for [assignment: *list of TSF functions*].

193 Refinement:

- a) If password generation algorithms are present, they shall meet the following requirements:
 - 1) The password generation algorithm shall generate passwords that are easy to remember (i.e., pronounceable).
 - 2) The TSF should give the user a choice of alternative passwords from which to choose.
 - 3) Passwords shall be reasonably resistant to brute-force password guessing attacks.
 - 4) If the “alphabet” used by the password generation algorithm consists of syllables rather than characters, the security of the password shall not depend on the secrecy of the alphabet.

- 5) The generated sequence of passwords shall have the property of randomness (i.e., consecutive instances shall be uncorrelated and the sequences shall not display periodicity).

FIA_UAU.1 Basic User Authentication

- 194 FIA_UAU.1.1 The TSF shall authenticate any user's claimed identity prior to performing any function for the user.

FIA_UAU.6 Configurable Authentication Mechanisms

- 195 FIA_UAU.6.1 The TSF shall provide [assignment: number] different mechanisms [assignment: list of different mechanisms] to authenticate any user's claimed identity.

- 196 FIA_UAU.6.2 The TSF shall enforce the use of [refinement: separate authentication mechanisms for specific authentication events], with authentication being successful if and only if all of the defined mechanisms individually indicate successful authentication.

- 197 FIA_UAU.6.3 The TSF shall allow the authorised administrator to associate [refinement: *separate authentication mechanisms with specific authentication events*].

FIA_UAU.9 Installable Authentication Mechanisms

- 198 FIA_UAU.9.1 The TSF shall provide the ability for the authorised administrator to incorporate installable authentication mechanisms into the TSF.

- 199 FIA_UAU.9.2 The TSF shall use the installed authentication mechanism in place of or in addition to any existing authentication mechanism.

FIA_UID.2 Unique Identification of Users

- 200 FIA_UID.2.1 The TSF shall uniquely identify each user before performing any actions requested by the user.

FIA_USB.1 User-Subject Binding

- 201 FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

3.5.1.2 TOE access requirements

FTA_LSA.1 Limitation on Scope of Selectable Attributes

- 202 FTA_LSA.1.1 The TSF shall restrict the scope of the session security attribute *role*, based on user identification.

- 203 FTA_LSA.1.2 Session establishment conditions shall be specifiable only by the authorised administrator.

FTA_MCS.2 Per User Attribute Limitation on Multiple Concurrent Sessions

204 FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that can operate on behalf of a user based on the user's identity.

205 FTA_MCS.2.2 The TSF shall enforce, by default, a limit of a single session per user.

206 FTA_MCS.2.3 When more than one user session security attribute is applicable, the TSF shall use the minimum number of sessions.

207 FTA_MCS.2.4 Session establishment conditions shall be specifiable only by the authorised administrator.

NOTE: At least one of the following two components shall be selected: FTA_SSL.1 (TSF-initiated Session Locking) or FTA_SSL.3 (TSF-initiated Termination). See note on these two components in section 3.7, Application notes.

FTA_SSL.1 TSF-initiated Session Locking

208 FTA_SSL.1.1 The TSF shall lock an interactive session after a specified interval of user inactivity by:

- a) clearing or overwriting display devices, making the current contents unreadable;
- b) disabling any activity of the user's data access/display devices other than unlocking the session.

209 FTA_SSL.1.2 The default value for the user inactivity interval shall be specifiable only by the authorised administrator.

210 FTA_SSL.1.3 The TSF shall require user authentication prior to unlocking the session.

FTA_SSL.3 TSF-initiated Termination

211 FTA_SSL.3.1 The TSF shall terminate an interactive session after a specified interval of user inactivity.

212 FTA_SSL.3.2 The default value for the user inactivity interval shall be specifiable only by the authorised administrator.

FTA_SSL.2 User-initiated Locking

213 FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive sessions by:

- a) clearing or over-writing display devices, making the current contents unreadable;

- b) disabling any activity of the user's data access/display devices other than unlocking the session.

214 FTA_SSL.2.2 The TSF shall require user authentication prior to unlocking the session;

FTA_TAB.2 Configurable TOE Access Banners

215 FTA_TAB.2.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

216 FTA_TAB.2.2 The default advisory warning message displayed by the TSF shall be as follows:

- a) NOTICE: This is a private computer system. All users of this system are subject to having their activities audited. Anyone using this system consents to such auditing. All unauthorised entries or activities revealed by this auditing can be used as evidence and may lead to criminal prosecution

217 FTA_TAB.2.3 The TSF shall restrict the capability to modify the warning message to the authorised administrator.

FTA_TAH.1 TOE Access History

218 FTA_TAH.1.1 Upon successful session establishment, the TSF shall display the date, time, method, and location of the last successful session establishment to the user.

219 FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the date, time, method, location of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

220 FTA_TAH.1.3 The data specified above shall not be removed without user intervention.

FTA_TAM.1 Basic TOE Access Management

221 FTA_TAM.1.1 The TSF shall restrict the capability to display and modify TOE access parameters to the authorised administrator.

222 FTA_TAM.1.2 The TSF shall allow the authorised administrators to display all TOE access parameters for a user, and users associated with a TOE access parameter.

FTA_TSE.1 TOE session establishment

223 FTA_TSE.1.1 The TSF shall be able to deny session establishment based on time of access.

224 Refinement:

- a) Entry conditions using these ranges shall be specified using time-of-day, day-of-week, and calendar dates.
- 225 FTA_TSE.1.1 The TSF shall be able to deny session establishment based on originating location.
- 226 FTA_TSE.1.1 The TSF shall be able to deny session establishment based on method of access.
- 227 FTA_TSE.1.2 Session establishment conditions shall be specifiable only by the authorised administrator.

3.5.1.3 Trusted path requirements

FTP_TRP.1 Trusted Path

- 228 FTP_TRP.1.1 The TSF shall provide a communication path between itself and local human users that is logically distinct from other communication paths and provides assured identification of its endpoints.
- 229 FTP_TRP.1.2 The TSF, and local users shall have the ability to initiate communication via the trusted path.
- 230 FTP_TRP.1.3 The TSF shall require initiation of the trusted path for initial user authentication, [assignment: *other services for which trusted path is required*]].

3.5.1.4 User data protection requirements

FDP_ACC.1 Subset Object Access Control - RBAC

- 231 FDP_ACC.1.1 The TSF shall enforce the Role-Based Access Control (RBAC) SFP on:
- a) subjects acting on behalf of users
 - b) [assignment: objects acted upon by RBAC operations]
 - c) [assignment: *RBAC operations performed on objects covered by the RBAC FSP*].
 - d) roles

FDP_ACF.1 Single Security Attribute Access Control - RBAC

- 232 FDP_ACF.1.1 The TSF shall enforce the RBAC SFP to objects based on the following subject attributes:
- a) user identity
 - b) role(s)

233 FDP_ACF.1.1 The TSF shall enforce the RBAC SFP to objects based on the following object attributes:

a) Object identifier.

234 FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

235 A subject operating in a role on behalf of a user can perform an operation on an object if:

a) The user is an authorised member of the role, and

b) The operation is an authorised operation for the role, and

c) The object is authorised for the operation.

FDP_ACF.3 Access Authorization - RBAC

236 FDP_ACF.3.1 The TSF shall enforce the RBAC SFP to provide the ability to explicitly grant access based on the value of security attributes of subjects and objects.

FDP_ACC.1 Subset Object Access Control -- DAC

237 FDP_ACC.1.1 The TSF shall enforce the Discretionary Access Control (DAC) SFP on:

a) subjects acting on behalf of users

b) [assignment: list of other subjects]

c) [assignment: list of objects]

d) [assignment: operations among subjects and objects covered by the DAC SFP, e.g., read, write, execute].

FDP_ACF.1 Single Security Attribute Access Control - DAC

238 FDP_ACF.1.1 The TSF shall enforce the DAC SFP to objects based on the following subject attributes:

a) user identity

b) groups of which the user is a member

239 FDP_ACF.1.1 The TSF shall enforce the DAC SFP to objects based on the following object attributes:

a) Access Control List: A list of user identities and/or a list of groups, and for each user identity and group entry, a list of permitted operations.

- b) A list of users and/or a list of groups that are explicitly denied access

240 FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

241 A subject is allowed to perform an operation on an object if:

- a) The subject's user identity is not on the list of users that are denied access to the object, and
- b) The subject's user identity is contained in the list of user identities of the object's ACL, or the user identity is a member of a group of the object's ACL, and the operation is contained in the list of operations for the user's identity.
- c) Denial of access takes precedence over granting of access.

FDP_ACF.4 Access Authorization and Denial

242 FDP_ACF.4.1 The TSF shall enforce the DAC SFP to provide the ability to explicitly grant access based on the value of security attributes of subjects and objects.

243 FDP_ACF.4.2 The TSF shall provide the ability to explicitly deny access based on the value of security attributes of subjects and objects covered.

FDP_ACI.3 Basic Attribute Initialisation

244 FDP_ACI.3.1 The TSF shall enforce the Discretionary Access Control SFP to provide restrictive default values for security attributes that are used to enforce the SFP.

245 FDP_ACI.3.2 The TSF shall allow the specification of alternate initial values to override the default values when an object is created.

246 FDP_ACI.3.3 The TSF shall provide authorised users the capability to modify the default values of their related attributes.

FDP_RIP.2 Full Residual Information Protection

247 FDP.RIP.2.1 The TSF shall ensure that upon the [selection: *allocation, deallocation, allocation or deallocation*] of a resource to/from all objects any previous information content is unavailable.

FDP_SAM.2 Basic Attribute Modification

248 FDP_SAM.2.1 The TSF shall enforce the Discretionary Access Control SFP to provide authorised users with the ability to modify access control lists created by the users.

FDP.SAM.3 Safe Attribute Modification

249 FDP.SAM.3.1 The TSF shall enforce the Role-Based Access Control SFP to verify that the modified values are valid when changes are made to the following:

- a) membership in roles,
- b) operations associated with roles,
- c) operations permitted for an object.

FDP_SAQ.1 Administrator Attribute Query

250 FDP_SAQ.1.1 The TSF shall enforce the Role-Based Access Control SFP to provide the authorised administrator with the ability to query the following attribute values:

- a) names of all roles,
- b) user members of a role,
- c) operations associated with a role,
- d) operations permitted on an object,
- e) objects accessible by a role.

FDP_SAQ.2 User Attribute Query

251 FDP_SAQ.2.1 The TSF shall enforce the Discretionary Access Control SFP to provide the authorised users with the ability to query the following attribute values:

- a) name of all groups,
- b) access control lists for objects that the user owns.

3.5.1.5 Audit requirements

FAU_ARP.1 Security Alarms

252 FAU_ARP.1.1 The TSF shall immediately generate an alarm to the authorised administrator upon detection of events deemed to indicate a possible security violation.

253 Refinement:

- a) When the threshold for incorrect attempted login sessions is exceeded, the TSF shall send an alarm message to the system console and/or to the administrator's terminal

FAU_ARP.2 Automatic Response

254 FAU_ARP.2.1 The TSF shall take [assignment: *the least disruptive actions*] to terminate the occurrence of a relevant security event upon detection of a possible security violation.

255 Refinement:

- a) The TSF shall end an attempted login session if the user performs the authentication procedure incorrectly for a number of successive times (i.e., a threshold) specified by the authorised administrator. The default threshold shall be three times.
- b) When the threshold is exceeded, the TSF shall delay the next login by an interval of time specified by the authorized system administrator. The default time interval shall be 60 seconds.
- c) The TSF shall provide a protected mechanism to disable the user identity or account when the threshold of successive, unsuccessful login attempts is violated more than a number of times specified by the administrator. By default, this mechanism shall be disabled (as it may cause unauthorized denial of service)

FAU_GEN.1 Audit Data Generation

256 FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions.
- b) All auditable events relevant for the basic level of audit as defined in all functional components included in the PP/ST.
 - 1) [FIA_ADA] Any attempts to use TSF authentication data management mechanisms.
 - 2) [FIA_ADP] Successful attempts to access user authentication data.
 - 3) [FIA_ADP] All attempts by an unauthorised user to access user authentication data.
 - 4) [FIA_ATA] All attempted uses of the user attribute administration function.
 - 5) [FIA_ATA] Identification of the user attributes that have been modified.
 - 6) [FIA_SOS] Rejection or acceptance by the TSF of any tested secret.
 - 7) [FIA_UAU] Any use of the authentication mechanism.
 - 8) [FIA_UAU] Audit the action of configuring the mapping of authentication mechanisms to specific authentication events.

- 9) [FIA_UAU] Installation of an authentication mechanism.
- 10) [FIA_UID] All attempts to use the user identification mechanism, including the user identity provided.
- 11) [FIA_USB] Success and failure of binding of user security attributes to a subject (e.g., creation of a subject).
- 12) [FTA_LSA] All attempts at selecting a user attribute based on the domain of selectable attributes.
- 13) [FTA_MCS] Rejection of a new session based on the limitation of multiple concurrent sessions.
- 14) [FTA_MCS] All attempts at establishment of a user session.
- 15) [FTA_SSL] Locking of an interactive session by the session locking mechanism.
- 16) [FTA_SSL] Successful unlocking of an interactive session.
- 17) [FTA_SSL] Termination of an interactive session by the session termination mechanism.
- 18) [FTA_TSE] All attempts at establishment of a user session.
- 19) [FTP_TRP] Identification of the initiator and target of the trusted channel.
- 20) [FTP_TRP] All attempted uses of the trusted channel functions.
- 21) [FDP_ACF] The security attributes used and the identity of any users, subjects, and/or objects involved in a successful mediation.
- 22) [FDP_ACF] Decisions to permit a requested operation.
- 23) [FDP_ACF] The security attributes used and the identity of any users, subjects, and/or objects involved in an unsuccessful mediation.
- 24) [FDP_ACF] Decisions to deny a requested operation.
- 25) [FDP_ACF] The identity of a user or subject unsuccessfully attempting to export an object.
- 26) [FDP_SAM] The identity of a user and/or subject successfully modifying security attributes and the target of the modification.
- 27) [FDP_SAM] Unsuccessful attempts to change security attributes.
- 28) [FDP_SAM] The new values of modified security attributes.

- 29) [FDP_SAM] The identity of a user and/or subject unsuccessfully attempting to modify security attributes, the target of the attempted modification, and the old and requested new value of the attribute.
- 30) [FDP_SAQ] The identity of a user successfully querying security attributes and the target of the query.
- 31) [FDP_SAQ] The identity of a user unsuccessfully querying security attributes and the target of the query.
- 32) [FAU_ARP] Generation of an alarm to the administrator when a security violation appears imminent.
- 33) [FAU_ARP] Successful application of the least disruptive action that should be taken when a security violation appears imminent.
- 34) [FAU_MGT] Any attempt to perform an operation on the audit trail.
- 35) [FAU_MGT] Notification of the authorised administrator in case of audit trail saturation.
- 36) [FAU_PAD] Enabling and disabling of any of the anomaly detection analysis mechanisms.
- 37) [FAU_PAD] Notifications made to the authorised administrator by the anomaly detection mechanisms.
- 38) [FAU_PAD] Automated responses made by the anomaly detection mechanisms.
- 39) [FAU_PAD] Any changes made to the configuration of the anomaly detection mechanisms.
- 40) [FAU_PIT] Enabling and disabling of any of the penetration identification analysis mechanisms.
- 41) [FAU_PIT] Notifications made to the authorised administrator by the penetration identification analysis mechanisms.
- 42) [FAU_PRO] Any attempt to read, modify, or destroy the audit trail.
- 43) [FAU_SAA] Detection of imminent violation by the security audit analysis mechanisms.
- 44) [FAU_SEL] All modifications to the audit configuration that occur while the audit collection functions are operating.
- 45) [FPT_SAE] Specification of the expiration time for a security attribute.
- 46) [FPT_TDC] Any use of the TSF data consistency mechanisms.
- 47) [FPT_TDC] Identification of which TSF data have been interpreted.

- 48) [FPT_TDC] Detection of modified TSF data.
- 49) [FPT_TSA] Use of a security-relevant administrative function.
- 50) [FPT_TSA] The designation of a function as a security-relevant administrative function.
- 51) [FPT_TSA] Explicit requests to assume the security administrative role.
- 52) [FRU_RSA] All attempted uses of the resource allocation functions for resources that are under the control of the TSF.
- c) Other auditable events defined below:
 - 1) [FPT_AMT] Use and result of the self test functions
 - 2) [FPT_TSA] [assignment: *actions taken by computer operators and system administrators and/or system security officers*]
 - 3) [assignment: *other auditable events*]

257 Refinement:

- a) The TSF shall support an application program interface that allows a privileged application to append data to the security audit trail or to an applications-specified alternative security audit trail.

258 FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity, and [selection: *success, failure*] of the event.
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

FAU_GEN.2 Individual Identity Generation

259 FAU_GEN.2.1 The TSF shall be able to associate any auditable events with the individual identity of the user that caused the events.

FAU_MGT.1 Audit Trail Management

260 FAU_MGT.1.1 The TSF shall provide the authorised administrator with the ability to [selection: *create, delete, empty*] the audit trail.

261 Refinement:

- a) The audit trail management tools shall enable:

- 1) Creation, destruction, and emptying of audit trails.
- 2) Modification of the audit trail size.
- 3) Formatting and compressing of event records.
- 4) Displaying of formatted audit trail data.
- 5) Automatic copying of security audit trail files to an alternative storage area after a system-specifiable period of time.
- 6) Automatic deletion of security audit trail files after a system-specifiable period of time. The default shall be thirty days.
- 7) It shall not be possible to delete the security audit trail before it gets copied to an alternate storage area. It shall be possible to disable this mechanism.
- 8) Maintaining the consistency of the audit trail data after system failures and discontinuity of operation.

FAU_MGT.3 Audit Trail Saturation Management

- 262 FAU_MGT.3.1 The TSF shall generate an alarm to the authorised administrator if the size of the audit data in the audit trail exceeds a pre-defined limit.
- 263 FAU_MGT.3.2 The TSF shall provide the authorised administrator with the ability to specify the pre-defined limit of the audit data in the audit trail at which point an alarm will be generated.

FAU_PAD.1 Profile Based Anomaly Detection

- 264 FAU_PAD.1.1 The TSF shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [assignment: *specify the profile target group*].
- 265 FAU_PAD.1.2 The TSF shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.
- 266 FAU_PAD.1.3 The TSF shall be able to indicate an imminent violation of the TSP when a user's suspicion rating exceeds the following threshold conditions [assignment: *conditions under which anomalous activity is reported by the TSF*].
- 267 Refinement:
- a) The TSF shall identify the number of successive incorrect attempted login sessions by a single user identity and compare that number against a threshold specified by an authorised administrator. The default threshold shall be three times.

FAU_PIT.1 Simple Attack Heuristics

268 FAU_PIT.1.1 The TSF shall be able to maintain an internal representation of the following signature events [assignment: *a subset of system events*] that may indicate a violation of the TSP.

269 Refinement:

- a) Successive incorrect login attempts by a single user identity.

270 FAU_PIT.1.2 The TSF shall be able to compare the signature events against the record of system activity discernable from an examination of [assignment: *specify the information to be used to determine system activity*].

271 Refinement:

- a) Audit records of failed login attempts.

272 FAU_PIT.1.3 The TSF shall be able indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.

FAU_PRO.2 Extended Audit Trail Access

273 FAU_PRO.2.1 The TSF shall restrict full access to the audit trail to the authorised administrator.

274 FAU_PRO.2.2 The TSF shall provide only authorised users with the capability to read [assignment: *list of audit information*] from the audit trail.

FAU_SAA.1 Imminent Violation Analysis

275 FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

276 FAU_SAA.1.2 The set of rules shall be:

- a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a possible or imminent security violation;
- b) Refinement:
Successive incorrect login attempts by a single user identity.
- c) [Assignment: *any other rules*].

FAU_SAR.2 Extended Audit Review

277 FAU_SAR.2.1 The TSF shall provide audit review tools, with the ability to view the audit data.

278 FAU_SAR.2.2 The TSF shall restrict full use of the audit review tools to the authorised administrator.

279 FAU_SAR.2.3 The TSF shall provide only authorised users with limited use of the audit review tools.

FAU_SEL.1 Selective Audit

280 FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

- a) [selection: *object identity, user identity, subject identity, host identity, event type*];
- b) [assignment: *list of additional attributes*] that audit selectivity is based upon.

FAU_SEL.2 Runtime Selection Mode

281 FAU_SEL.2.1 The TSF shall provide the authorised administrator with the capability to select, at any time during the operation of the TOE, which events are to be audited.

FAU_SEL.3 Restricted Runtime Display Mode

282 FAU_SEL.3.1 The TSF shall restrict to the authorised administrator the capability to display, at any time during the operation of the TOE, which events are being audited.

FAU_STG.1 Permanent Audit Trail Storage

283 FAU_STG.1.1 The TSF shall store generated audit records in a permanent audit trail.

FAU_STG.3 Prevention of Audit Data Loss

284 FAU_STG.3.1 The TSF shall limit the number of audit records lost due to system [selection: *audit storage exhaustion, failure, attack*].

285 FAU_STG.3.2 In the event of audit storage exhaustion, the TSF shall be capable of [selection: *ignoring, preventing*] the occurrence of auditable actions, except those taken by the authorised administrator.

3.5.1.6 Protection of trusted security functions requirements

FPT_AMT.3 Abstract Machine Testing During Normal Operation

286 FPT_AMT.3.1 The TSF shall provide the authorised administrator with the capability to demonstrate the correct operation of the security-relevant functions provided by the TSF's underlying abstract machine.

287 FPT_AMT.3.2 The TSF shall run a suite of self tests during initial start-up and periodically during normal operation in order to demonstrate the correct operation of the functions provided by the TSF's underlying abstract machine.

FPT_FLS.1 Failure with Preservation of Secure State

288 FPT_FLS.1.1 The TSF shall preserve secure state when [assignment: *list of types of TSF failures.*] failures occur:

FPT_PHP.1 Passive Detection of Physical Attack

289 FPT_PHP.1.1 The TOE shall include features that provide unambiguous detection of physical tampering with the TSFs physical devices and elements.

290 FPT_PHP.1.2 The TSF shall provide the authorised administrator with the capability to determine whether physical tampering to the TSF's devices and elements has been detected.

FPT_RCV.2 Automated Recovery

291 FPT_RCV.2.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

292 FPT_RCV.2.2 The TSF shall provide the authorised administrator with the capability to restore the TSF data to a consistent and secure state.

293 FPT_RCV.2.3 For [assignment: *list of failures/service discontinuities*], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RVM.1 Non-Bypassability of the TSP

294 FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before any security-related action is allowed to proceed.

FPT_SAE.1 Time-Limited Authorisation

295 FPT_SAE.1.1 The TSF shall provide a capability for the authorised administrator to specify an expiration time for [assignment: *list of security attributes for which expiration is to be supported*].

296 FPT_SAE.1.2 For each of these security attributes, the TSF shall be able to [assignment: *list of actions to be taken for each security attribute*] after the expiration time for the indicated security attribute has passed.

297 Refinements:

- a) The TSF shall enforce password aging on a per- user identifier, per-group, or per-role basis (i.e., a user shall be required to change his or her password after a system-specifiable minimum time). The default for all non-system administrators shall be sixty days.
- b) The default for system administrator identifiers shall be thirty days.
- c) After the password aging threshold has been reached, the password shall no longer be valid, except as provided in 5 g below.

- d) The TSF shall provide a protected mechanism to notify users in advance of requiring them to change their passwords. This can be done by either:
 - 1) Notifying users a system-specifiable period of time prior to their password expiring. The default shall be seven days.
 - or -
 - 2) Upon password expiration, notifying the user but allowing a system-specifiable subsequent number of additional logons prior to requiring a new password. The default shall be two additional logons.
- e) The control of user password expiration defaults shall be limited to system administrators.

FPT_SEP.1 TSF Domain Separation

298 FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

299 FPT_SEP.1.2 The TSF shall enforce separation between the address spaces of subjects in the TSC.

FPT_SWM.1 Protection of Executables

300 FPT_SWM.1.1 The TSF shall provide the authorised administrator with the capability to verify the integrity of stored TSF executable code.

FPT_TDC.1 Inter-TSF Basic TSF Consistency

301 FPT_TDC.1.1 The TSF shall enforce the consistent interpretation of [assignment: *list of TSF data types*] during inter-TSF transfers.

302 FPT_TDC.1.2 The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data during inter-TSF transfers.

FPT_TSA.2 Separate Security Administrative Roles

303 FPT_TSA.2.1 The TSF shall distinguish security-relevant administrative functions from other functions.

304 FPT_TSA.2.2 The TSF's set of security-relevant administrative functions shall include all functions necessary to install, configure, and manage the TSF; minimally, this set shall include [assignment: *list of services to be minimally supplied*].

305 FPT_TSA.2.3 The TSF shall restrict the ability to use security-relevant administrative functions to a security administrative role that has a specific set of authorised functions and responsibilities.

306 FPT_TSA.2.4 The TSF shall be capable of distinguishing the set of users authorised for administrative functions from the set of all users of the TOE.

307 FPT_TSA.2.5 The TSF shall allow only specifically authorised users to assume the security administrative role.

308 FPT_TSA.2.6 The TSF shall require an explicit request to be made in order for an authorised user to assume the security administrative role.

FPT_TSM.1 Management Functions

309 FPT_TSM.1.1 The TSF shall provide the authorised administrator with the ability to set and update the following TSF configuration parameters:

- a) The authentication method on a per policy-attribute basis whenever multiple authentication methods are used for FIA_UAU
- b) Session establishment conditions to limit the scope of selectable attributes for FTA_LSA.1..
- c) Per user attribute limitations on multiple concurrent sessions for FTA_MCS.2
- d) The default value for the user activity interval for FTA_SSL.1 or FTA_SSL.3
- e) The warning message for FTA_TAB.2
- f) The time of access, originating of access, and method of access conditions for FTA_TSE.1
- g) The audit trail parameter for FAU_MGT.1
- h) The pre-defined limit of the audit data in the audit trail for FAU_MGT.3.
- i) assignment: [*other TSF configuration parameters*].

310 FPT_TSM.1.2 The TSF shall provide the authorised administrator with the ability to perform the following administrative functions:

- a) Create named groups.
- b) Delete named groups
- c) Authorise users into one or more named groups.
- d) Create named roles.
- e) Delete named roles.
- f) Authorise users into one or more named roles.
- g) Authorise one or more role operations for a role.

- h) Authorise one or more operations that can be performed on a role.
- i) [assignment: *other administrative functions*].

FPT_TST.3 TSF Testing During Normal Operation

- 311 FPT_TST.3.1 The TSF shall provide authorised administrators with the capability to demonstrate the correct operation of the TSF.
- 312 FPT_TST.3.2 The TSF shall provide authorised administrators with the capability to verify the integrity of TSF data.
- 313 FPT_TST.3.3 The TSF shall exercise a suite of self tests during initial start-up and periodically during normal operation in order to demonstrate the correct operation of the TSF.
- 314 Refinements:
 - a) Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TSF. These features shall include: power-on tests, loadable tests, and operator-controlled tests.
 - b) The power-on tests shall test all basic components of the TSF hardware and firmware elements including memory boards and memory interconnections; data paths; busses; control logic and processor registers; disk adapters; communication ports; system consoles, and the keyboard speaker. These tests shall cover all components that are necessary to run the loadable tests and the operator-controlled tests.
 - c) The loadable tests shall cover: processor components (e.g., arithmetic and logic unit, floating point unit, instruction decode buffers, interrupt controllers, register transfer bus, address translation buffer, cache, and processor-to-memory bus controller); backplane busses; memory controllers; writable control memory for operator-controlled and remote system-integrity testing.
 - d) Operator-controlled tests shall be able to initiate a series of one-time or repeated tests, to log the results of these tests and, if any fault is detected, to direct the integrity-test programs to identify and isolate the failure. The execution of operator-controlled tests shall be limited to system operators.

FPT_TSU.1 Enforcement of Administrative Guidance

- 315 FPT_TSU.1.1 The TSF shall enforce checks for valid input values for security-relevant administrative functions as described in the Administrative Guidance.

FRU_RSA.1 Maximum Quotas

- 316 FRU_RSA.1.1 The TSF shall enforce quotas limiting the maximum quantity of [assignment: *controlled resources*] that [selection: *individual user, defined group of users*] can use [selection: *simultaneously, over a specified period of time*].

3.5.2 Assurance requirements

- 317 The assurance requirements for CS3 are portrayed in Table 3.2 below. The assurance augmentation components are described following the table.

Requirement	Name
EAL4	Methodically Designed, Tested, and Reviewed
ALC_FLR.2	Flaw Reporting Procedures
ADO_DEL.2	Detection of Modification

Table 3.2 - CS3 assurance requirements

ALC_FLR.2 Flaw reporting procedures

- 318 Dependencies: AGD_ADM.1 Administrator Guidance (in EAL4).
- 319 Developer action elements:
- a) ALC_FLR.2.1D The developer shall document the flaw remediation procedures.
 - b) ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon user reports of security flaws and requests for corrections to those flaws.
- 320 Content and presentation of evidence elements:
- a) ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
 - b) ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
 - c) ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
 - d) ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information and corrections to TOE users.
 - e) ALC_FLR.2.5C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

321 Evaluator action elements:

- a) ALC_FLR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_DEL.2 Detection of modification

322 Dependencies: ACM_CAP.2 Authorisation controls (covered by ACM_CAP.3 in EAL4).

323 Developer action elements:

- a) ADO_DEL.2.1D The developer shall provide documentation about the procedures for delivery of the TOE or parts of it to the user.
- b) ADO_DEL.2.2D The developer shall use the delivery procedures.

324 Content and presentation of evidence elements:

- a) ADO_DEL.2.1C The delivery documentation shall describe the procedures to be employed when distributing versions of the TOE to a user site.
- b) ADO_DEL.2.2C The delivery documentation shall state how the procedures are to be employed to detect modifications.
- c) ADO_DEL.2.3C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.
- d) ADO_DEL.2.4C The delivery documentation shall describe how the various procedures allow detection of attempted masquerading even in cases in which the developer has sent nothing to the user's site.

325 Evaluator action elements:

- a) ADO_DEL.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

3.6 Environmental IT security requirements

326 CS3 is primarily applicable to TOEs which are fully responsible for enforcement of the TOE Security Policy (TSP) and do not, therefore, require that the IT environment of the TOE accept any TSP enforcement responsibility.

327 Application of CS3 to a TOE which requires some of the CS3 IT security requirements to be met by the TOE IT environment is permissible. Should this be the case, the Security Target must explain the partition of security requirements

between the TOE and its IT environment and demonstrate that the TOE in its IT environment satisfies all of the CS3 security requirements.

3.7 Application notes

- 328 FIA_SOS.1, Selection of Secrets, applies TOE constraints to the administration of user-generated passwords. It should only be included in the PP if the TOE has the capability for using user-generated passwords for user identification and authentication.
- 329 FIA_SOS.2, TSF Generation of Secrets, applies quality metrics to the process of generating passwords by the TSF. It should only be included in the PP if the TOE has the capability for generating passwords for user identification and authentication.
- 330 FTA_SSL.1, TSF-initiated Session Locking, and FTA_SSL.3, TSF-initiated Termination, both require the TSF to take some action against an interactive session after a specified interval of user inactivity. At least one of these two components shall be selected for the TOE, although it is permissible to select both as that could provide the authorised administrator with the option of using either one according to need.
- 331 TOEs that comply with CS3 are intended to be used within the following operational constraints:
- a) The information system is designed to be administered as a unique entity by a single organisation.
 - b) The information system is designed to manage computing, storage, input/output, and to control the sharing of resources among multiple users and processes.
 - c) The information system provides facilities for interaction with users who have access to input/output devices.
 - d) The administrative and non-administrative users are distinct individuals.
 - e) System administrators are responsible for interpreting and enforcing organisational policies and protection guidelines.
 - f) System administrators and users are selectively assigned security related privileges that are minimally necessary to perform their tasks.

Chapter 4

Network/Transport Layer Packet Filter Firewall (PFFW) PP

4.1 Introduction

4.1.1 Identification

332 Title: Network/Transport Layer Packet Filter Firewall - PFFW

333 Registration: <to be filled in on registration>

334 Keywords: Access control, firewall, packet filter, network layer, transport layer, OSI, TCP, IP, IPX, SPX

4.1.2 Protection Profile overview

335 The intent of this Protection Profile is to specify functions and assurances applicable to most commercially available packet filter firewalls. The intent of this profile is more focused on reflecting current market practices, rather than mandating security functions not already present in most products. The sole exception may be slightly stronger auditing functions than currently available, to reflect increased user demands for accountability and monitoring of their network connections. Although most commercially available products are targeted at the TCP/IP protocol stack, there is nothing inherent in the requirements as stated that mandate a compliant firewall to use that protocol stack. The purpose of a packet filter firewall is to provide a point of defence and controlled and audited access to services, both from within and outside an organisation's private network, by permitting and/or denying the flow of packets through the firewall.

4.2 TOE description

336 A typical arrangement including a firewall that complies with this profile is described in Figure 4.1. The firewall is installed between two networks so that traffic between them must be routed through the firewall. The firewall can thus provide access control based upon packets being routed between the networks. A

firewall is a computing device (e.g., router or host) that is used to physically separate one network domain from another.

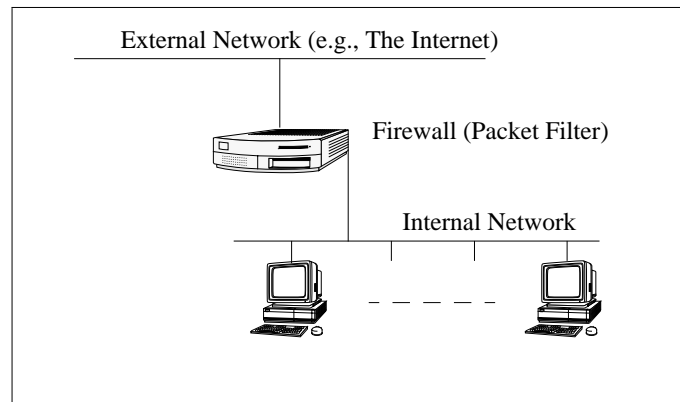


Figure 4.1 - Typical firewall location in a network environment

337 Routers can control traffic at the network/transport layer by selectively permitting or denying traffic based on source/destination address or port. Hosts can control traffic at an application level. This Protection Profile addresses a network/transport-layer packet-filtering operation concept. An example would be a firewall that performs security decisions based on information in both IP and TCP headers (e.g., source address and port).

4.3 Security environment

4.3.1 Summary

338 Compliant firewalls are intended for use in commercial environments wishing to have flexible access control policies, some auditing capability, and a minimal level of assurance in the security functions.

4.3.2 Threats to security

339 This Protection Profile is sufficient for relatively benign physical and operational environments where the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate. The intent of this profile is to control access to services, thereby limiting the ability to gain unauthorised access to the protected network or networks. Thus, the primary threats countered are those of errors or casual attempts to violate the security policy enforced by the TSF.

4.3.2.1 Threats addressed by the TOE

340 The possible threats discussed below are addressed by PP-compliant firewalls.

T.LACCESS An unauthorised person may gain logical access to the firewall.

341 The term unauthorised person is used to cover all those persons who have, or may attempt to gain, logical access to the firewall but have no authority to gain logical access to the firewall or perform operations on its information.

T.SPOOF An unauthorised person may carry out network address spoofing attacks (e.g., IP spoofing) from one network connection to another, traversing the firewall.

342 The general model used is that the firewall provides access control between one or more “external” (untrustworthy) networks, and one or more “internal” (or “private”, trustworthy) networks. The specific threat countered is a subject on an external network attempting to masquerade as a subject on an internal network.

T.SACCESS An unauthorised person may carry out attacks on services.

343 The specific threats countered depend on the protocols allowed to pass through the firewall. A service that cannot be accessed from outside the internal network does not pose a threat. Threats that do not originate from the traffic through the firewall are specifically not addressed in this profile.

T.SOURCE An unauthorised person may carry out source routing-type attacks at the network layer.

344 Various network-layer protocols allow the originator of a packet to specify the path that a packet will traverse from source to destination. In some routing implementations, if source routing is indicated in the protocol header, the protocol processing function will bypass any rule checks, thus offering an unintended avenue to “tunnel through” a firewall performing a routing function.

T.PENET An unauthorised person may carry out undetected penetration attempts.

345 An unauthorised person may be able to repeatedly try different attacks against a network to be protected without personnel on the attacked network being aware that such attempts are taking place.

T.AUDITREV There may be lack of audit trail review.

346 Even if audit data are collected, if these data are not reviewed, either because of the quantity of data generated or lack of adequate review tools, an attacker may be able to escape detection while performing repeated penetration attempts.

T.ACORR An attacker may corrupt the audit trail.

347 This threat is two-fold. First, an attacker could directly corrupt the audit trail by manipulating it through an interface at the firewall (e.g., a specific control protocol going over the network). The second threat is that an attacker could crash the firewall after performing a penetration or attempted penetration, and if the audit

trail is not sufficiently protected it could possibly get lost, thus masking the attacker's actions.

T.DCORR An attacker may modify the firewall configuration and other security-relevant data.

348 This threat is similar to T.ACORR, except that the data that are targeted by an attacker are firewall configuration and other security-critical data.

T.FLAW Security failures may occur because of flaws in the firewall.

349 The security offered can be assured only to the extent that all of the security features can be trusted to be effective in countering the threats and to operate correctly and reliably.

350 Threat agents may, through accidental discovery or directed search, discover flaws in the firewall which may be subverted such that the operation of the security functions is changed to their advantage.

351 Such subversion of the firewall may occur during delivery and installation. During normal operation, potential attackers may also seek to develop methods whereby the security functions may be undermined.

4.3.2.2 Threats to be addressed by operating environment

352 The possible threats discussed below are *not* addressed by PP-compliant firewalls. They must either be countered by the environment, procedural means, or accepted as potential system risks.

T.EVIL_ADM There are careless, wilfully negligent, or hostile system administration personnel.

353 Since administrators are responsible for setting the access control rules and for monitoring the audit trail, they will be able to trivially circumvent the security mechanisms of the firewall.

T.INSHARE Hostile users on a protected network ("behind" the firewall) wish to share information with users on an external network.

354 This threat deals with the case that a user on an internal (protected) network wishes to illegitimately send information to a user on an external network. Since this firewall PP is specifically designed to protect internal networks from external networks and is not intended to check the content of the packet, it will be generally ineffective against these kinds of attacks.

T.INALL Hostile users on a protected network attack machines that are part of the protected network.

355 Since a firewall by definition is to protect users on an internal network from users external to the network it cannot protect from attacks not targeted at the firewall.

T.SERVICES Hostile users on a protected network try to carry out sophisticated attacks on higher-level protocols and services.

356 These types of attacks target flaws in protocol layers (and services using those protocols) above the transport layer. The firewall may be able to completely deny packets to specific services, but once packets are allowed to pass, then attacks on the services they are targeted for may be possible. The firewall is not required to check the content of the packet.

4.3.3 Organisational security policies

357 Although compliant firewalls can be used as to satisfy some organisational security policies, no specific examples are specified here.

358 An organisational security policy could be based on all information that is available on the packet level, (e.g., network addresses). However, the content of the packet is not required to be examined.

4.3.4 Secure usage assumptions

359 The following specific conditions are assumed to exist in the firewall's operational environment.

4.3.4.1 Physical assumptions

360 It is assumed that the following physical conditions will exist:

A.SECURE The firewall and associated directly-attached consoles is physically secure, i.e. access is limited to authorised personnel only.

A.DIRCON Authorised personnel (administrators) interact with the firewall only through directly-attached consoles, i.e. no network "login" is permitted for administrators.

A.TRANSP The firewall does not require changing the operating properties (e.g., software applications, hardware) on either the internal network or the external network to operate.

4.3.4.2 Personnel assumptions

361 It is assumed that the following personnel conditions will exist:

A.NO_USER The firewall is designed solely to act as a firewall and does not provide additional user services (e.g., login) to any users on the internal or external network; only administrators have direct access.

A.NO_EVIL Administrators are assumed to be non-hostile and trusted to perform their duties correctly.

4.3.4.3 Connectivity assumptions

362 It is assumed that the following connectivity conditions exist:

A.SINGL_PT The firewall is the only interconnection device between networks.

363 In Figure 4.2., two architectures are illustrated. The left architecture provides an allowed configuration. On the right hand side, an example of a disallowed architecture is provided.

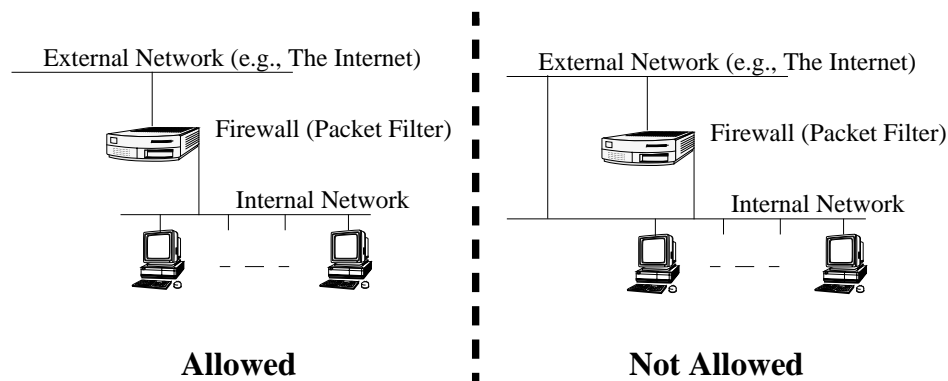


Figure 4.2 - Allowed and disallowed connections for compliant firewalls

4.4 Security objectives

4.4.1 IT security objectives

364 The following are the TOE/firewall IT security objectives:

O.ACCESS The firewall must provide controlled access between networks connected to it by permitting or denying the flow of packets.

365 The decision to allow or deny a packet to pass through the firewall is based on attributes of the subject, object, possibly firewall-generated state information, and administratively configured access control rules.

366 Since the firewall only operates on the packet level there can be no human users of the firewall in the generally understood sense of the word 'user'. Any identification and authentication information would be part of the content the packet carries forward and is therefore out of the TSC. The administration personnel directly access the firewall through the console and are authenticated via the procedures that allow permission to physically access the firewall (see A.SECURE).

367 Therefore the concept of machine users is applied. A machine user (identified as TCP/IP port on another machine) is represented in the TSF either as a subject or an object. Subjects and objects are identified by the source and destination information the packet contains. Except for the authorised administrator, each reference to a user refers to the machine user on the TCP/IP port as identified in a packet. A user to subject binding to hold a human user accountable for the actions on the packets is out of the TSC.

O.ADMIN The firewall must limit the direct access to it to a directly attached console.

368 This objective limits the access to the firewall to authorised, administrative personnel, and gives only those individuals the ability to configure the firewall (see also A.NO_USER). This access is mediated by the directly attached console. This objective is closely related to, and supports, O.AUDIT.

O.PROTECT The firewall must be able to separate data that it needs to operate (TSF data) from data that it is processing (packets).

369 The firewall must prevent itself from being attacked by external entities. This includes the protection of executable code as well as protection of packets actually processed. The protection of the audited data also fits into this enumeration.

O.AUDIT The firewall must ensure that all users can subsequently be held accountable for their security relevant actions (see also O.ACCESS).

370 An audit trail is necessary to determine if there are ongoing attempts to circumvent the implementation of the security policy, or if there are misconfigurations of the firewall that unwittingly allow access where it should be denied. Not only must the audit data be collected, but it must be viewable and relatively easy to work with. Finally, the audit trail must be sufficiently protected and the scope of potential audit record loss known so that sound security decisions by administrative personnel can be supported.

O.FLAW The firewall must be developed in order not to contain flaws in design or implementation.

371 This objective specifically addresses the assurance requirements part of this PP.

4.4.2 Non-IT security objectives

372 The firewall is assumed to be complete and self-contained, and as such is not dependent upon any other products to perform properly (see A.TRANSP).

However, certain objectives with respect to the operating environment must be met in order to support the firewall's security capabilities.

373 The following are the non-IT security objectives:

O.INSTALL Those responsible for the firewall must ensure that it is delivered, installed, managed, and operated in a manner which maintains the system security.

374 It must be sure that the firewall delivered is an identical copy of the one evaluated. During installation all security services necessary for security maintaining operation must be switched on. The management and operation must also maintain security, e.g. by user training and motivation. This is closely related to the threat of hostile administration personnel (see T.EVIL_ADM).

O.PACCESS Those responsible for the firewall must ensure that physical access to it is controlled.

375 As the firewall itself does not carry out identification and authentication of the administration personnel the operational conditions must ensure that only the administration personnel have admittance to the physical environment of the firewall. For subject/object identification (needed for the establishment of access control rules) the firewall relies on requirements that must be met by the environment, e.g. user to subject binding.

O.TRAIN Those responsible for the firewall must ensure that administrators have the necessary skills in establishment and maintenance of sound security policies and practices.

376 No assumptions are made on how the administration personnel must be trained. It must be sure that the appropriate skills are present before the firewall begins to operate. The administration personnel are assumed to have an appropriate sense of responsibility.

4.5 TOE IT security requirements

4.5.1 Functional requirements

377 The following Table summarises the functional components included in this PP.

FAU_GEN.1	Audit Data Generation
FAU_MGT.1	Audit Trail Management
FAU_POP.1	Human Understandable Format
FAU_PRO.1	Restricted Audit Trail Access
FAU_SAR.1	Restricted Audit Review

Table 4.1 - Functional Components

FAU_SAR.3	Selectable Audit Review
FAU_STG.3	Prevention of Audit Data Loss
FIA_ADA.1	User Authentication Data Administration
FIA_ADP.1	Basic User Authentication Data Protection
FIA_ATA.1	User Attribute Initialisation
FIA_ATD.1	Shared User Attribute Definition
FIA_UAU.1	Basic User Authentication
FIA_UID.1	Basic User Identification
FIA_USB.1	User-Subject Binding
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
FPT_TSA.1	Basic Security Administration
FPT_TSM.1	Management Functions
FDP_ACC.2	Complete Object Access Control
FDP_ACF.2	Multiple Security Attribute Access Control
FDP_ACF.4	Access Authorisation and Denial
FDP_ACI.1	Static Attribute Initialisation
FDP_ETC.1	Export of User Data Without Security Attributes
FDP_ITC.1	Import of User Data Without Security Attributes
FDP_SAM.1	Administrator Attribute Modification
FDP_SAQ.1	Administrator Attribute Query

Table 4.1 - Functional Components**FAU_GEN.1 Audit Data Generation**

378 FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions;
- b) All auditable events relevant for the minimum level of audit as defined in all functional components included in the PP/ST (see Table 2.4); and
- c) Based on all functional components included in the PP/ST, [Assignment: *other auditable event as specified by the ST author*].

379 FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity, and failure of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, the attributes presented in brackets in Table 2.4 should be included..

Component	Event
FAU_GEN.1	failure of start-up
FAU_MGT.1	unsuccessful operations on the audit trail
FAU_POP.1	any specific operation performed to process audit data stored in the audit trail.
FAU_PRO.1	successful requests to read, modify or destroy the audit trail.
FAU_SAR.1	----
FAU_SAR.3	---
FAU_STG.3	audit storage exhaustion
FIA_ADA.1	successful use of any TSF authentication data management mechanisms.
FIA_ADP.1	successful requests to access user authentication data.
FIA_ATA.1	successful use of the user attribute administration functions
FIA_ATD.1	---
FIA_UAU.1	successful use of the authentication mechanism
FIA_UID.1	successful use of the user identification mechanism, including the user identity provided
FIA_USB.1	successful binding of user security attributes to a subject
FPT_RVM.1	---
FPT_SEP.1	---
FPT_TSA.1	use of a security-relevant administrative function
FPT_TSM.1	successful and unsuccessful attempts to modify (set and update) TSF configuration parameters.
FDP_ACC.2	---
FDP_ACF.2	successful attempts to access an object covered by the firewall flow policy
FDP_ACF.4	---
FDP_ACI.1	successful changes to default values successful overriding of the default values
FDP_ETC.1	successful export of information.
FDP_ITC.1	successful import of information
FDP_SAM.1	successful modification of the security attributes [target of the modification].
FDP_SAQ.1	successful query on the security attributes [target of the query]

Table 4.2 - Auditable events

FAU_MGT.1 Audit Trail Management

380 FAU_MGT.1.1 The TSF shall provide the authorised administrators with the ability to create, delete, and empty the audit trail.

FAU_POP.1 Human Understandable Format

381 FAU_POP.1.1 The TSF shall be able to generate a human understandable presentation of any audit data stored in the permanent audit trail.

FAU_PRO.1 Restricted Audit Trail Access

382 FAU_PRO.1.1 The TSF shall restrict access to the audit trail to the authorised administrator.

FAU_SAR.1 Restricted Audit Review

383 FAU_SAR.1.1 The TSF shall provide audit review tools, with the ability to view the audit data.

384 FAU_SAR.1.2 The TSF shall restrict use of the audit review tools to authorised administrators.

FAU_SAR.3 Selectable Audit Review

385 FAU_SAR.3.1 The TSF shall provide audit review tools with the ability to perform searches and sorting of audit data based on [Assignment: *multiple criteria with logical relationships as specified by the ST author*].

FAU_STG.3 Prevention of Audit Data Loss

386 FAU_STG.3.1 The TSF shall store generated audit records in a permanent audit trail.

387 FAU_STG.3.2 The TSF shall limit the number of audit records lost due to audit storage exhaustion, failure, and attack.

388 FAU_STG.3.2 In the event of audit storage exhaustion, the TSF shall be capable of [selection: ignoring, preventing as specified by the ST author] the occurrence of auditable actions, except those taken by the authorised administrator.

FIA_ADA.1 User Authentication Data Initialisation

389 FIA_ADA.1.1 The TSF shall provide functions for initialising user authentication data related to passwords.

390 FIA_ADA.1.2 The TSF shall restrict the use of these functions to the authorised administrator.

FIA_ADP.1 Basic User Authentication Data Protection

391 FIA_ADP.1.1 The TSF shall protect from unauthorised observation, modification, and destruction authentication data that is stored in the TOE.

FIA_ATA.1 User Attribute Initialisation

392 FIA_ATA.1.1 The TSF shall provide the ability to initialise user attributes with provided default values.

FIA_ATD.1 Shared User Attribute Definition

393 FIA_ATD.1.1 The TSF shall provide, for each user, a set of security attributes necessary to enforce the TSP.

FIA_UAU.1 Basic User Authentication

394 FIA_UAU.1.1 The TSF shall authenticate the authorised administrator's claimed identity prior to performing any functions for the authorised administrator.

FIA_UID.1 Basic User Identification

395 FIA_UID.1.1 The TSF shall identify each user before performing any actions requested by the user.

FIA_USB.1 User-Subject Binding

396 FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

FPT_RVM.1 Non-Bypassability of the TSP

397 FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before any security-related operation is allowed to proceed.

FPT_SEP.1 TSF Domain Separation

398 FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

399 FPT_SEP.1.2 The TSF shall enforce separation between the security domains in the TSC.

FPT_TSA.1 Basic Security Administration

400 FPT_TSA.1.1 The TSF shall distinguish security-relevant administrative functions from other functions.

401 FPT_TSA.1.2 The TSF's set of security-relevant administrative functions shall include all functions necessary to install, configure, and manage the TSF; minimally, this set shall include the following services:

- a) administrator security attribute maintenance including default setup and overriding;
- b) audit function maintenance including start-up, shutdown;
- c) creation, deletion and emptying of audit trail;
- d) audit review tools;
- e) initialising user authentication data;
- f) modifying and displaying the firewall flow control parameters (access control parameters).
- g) [Assignment: *other services as specified by the ST author*].

402 FPT_TSA.1.3 The TSF shall restrict the ability to perform security-relevant administrative functions to specifically authorised users.

403 FPT_TSA.1.4 The TSF shall be capable of distinguishing the set of users authorised for administrative functions from the set of all users of the firewall.

FPT_TSM.1 Management Functions

404 FPT_TSM.1.1 The TSF shall provide the authorised administrators with the ability to set and update the following TSF configuration parameters:

- a) the access control parameters;
- b) default user attributes;
- c) audit rules;
- d) [Assignment: *others as specified by the ST author*].

405 FPT_TSM.1.2 The TSF shall provide the authorised administrators with the ability to:

- a) provide security attribute maintenance including default setup and overriding;
- b) manage the audit function including start-up, shutdown;
- c) provide creation, deletion and emptying of audit trail.
- d) review the audit data;

- e) initialise user authentication data;
- f) manage user, subject and object attributes;
- g) modify and display the firewall flow control parameters (access control parameters);
- h) manage interfaces;
- i) [Assignment: *allow enabling and disabling of the set of peripheral devices specified by the ST author*].

FDP_ACC.2 Complete Object Access Control

406 FDP_ACC.2.1 The TSF shall enforce the firewall flow policy on the subjects and objects and all operations among subjects and objects covered by the firewall flow policy (e.g., write operation).

407 FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by the firewall flow policy.

FDP_ACF.2 Multiple Security Attribute Access Control

408 FDP_ACF.2.1 The TSF shall enforce the firewall flow policy to objects based on:

- 409 a) network identification of the subject and the object;
- 410 b) identity of the subject (e.g., TCP/IP address);
- 411 c) identity of the object (e.g., TCP/IP address);
- 412 d) time.

413 FDP_ACF.2.2 The TSF shall enforce the following rule to determine if an operation among controlled subjects and controlled objects is allowed:

- 414 a) if the time is between a period specified by the authorised administrator; and
- 415 b) either the subject or the object has an internal network identification, and the other one has an external network identification; and
- 416 c) if the subject is known to be connected to the internal network, the port to which the subject is connected must be an internal network; and
- 417 d) access between the subject and object identity is explicitly allowed; and
- 418 e) access between the subject and object identity is not explicitly disallowed in a subset of the groups which allowed the operation (e.g., all users on a network are allowed to do action X, except all users whose port is located on number 25),

419 then the operation is allowed.

FDP_ACF.4 Access Authorisation and Denial

420 FDP_ACF.4.1 The TSF shall enforce the firewall flow policy to provide the ability to explicitly grant access based on the value of security attributes of subjects and objects.

421 FDP_ACF.4.1 The TSF shall enforce the firewall flow policy to provide the ability to explicitly deny access based on the value of security attributes of subjects and objects.

FDP_ACI.1 Static Attribute Initialisation

422 FDP_ACI.1.1 The TSF shall enforce the firewall flow policy to provide restrictive default values for object security attributes that are used to enforce the firewall flow policy.

423 FDP_ACI.1.2 The TSF shall allow the specification of alternate initial values to override the default values when an object is created.

FDP_ETC.1 Export of User Data Without Security Attributes

424 FDP_ETC.1.1 The TSF shall enforce the firewall flow policy for information exported outside the TSC via a function that does not provide the information's corresponding security attributes.

FDP_ITC.1 Import of User Data Without Security Attributes

425 FDP_ITC.1.1 The TSF shall enforce the firewall flow policy for information imported from outside the TSC by the TSF via a function that does not provide reliable security attributes.

426 The TSF shall allow an authorised user to supply the security attributes for the information received.

427 FDP_ITC.1.2 The TSF shall provide the following rules:

- a) the user identity will be set to the originator information in the packet;
- b) the object identity will be set to the destination indicated in the packet;
- c) the subject network will be set to the port on which the information was received;
- d) the object network will be set to the port on which the destination is connected

428 when information controlled under the firewall flow policy is imported from outside the TSC.

FDP_SAM.1 Administrator Attribute Modification

429 FDP_SAM.1.1 The TSF shall enforce the firewall flow policy to provide authorised administrators with the ability to modify the [Assignment: *firewall flow control parameter as specified by the ST author*].

FDP_SAQ.1 Administrator Attribute Query

430 FDP_SAQ.1.1 The TSF shall enforce the firewall flow policy to provide the authorised administrator with the ability to query the [Assignment: *firewall flow control parameter as specified by ST author*] values.

4.5.2 Assurance requirements

431 The assurance requirements consist of EAL1 - functionally tested.

4.6 Environmental IT security requirements

432 The firewall is assumed to be complete and self-contained and, as such, is not dependent upon any other products to perform properly (see A.TRANSP).

4.7 Application notes

433 In a typical packet-filtering firewall, there are two or more physical interfaces against which rules can be applied. The purpose of the rules is to either allow or deny packets to flow through the firewall. Most firewalls (at least those with exactly two interfaces) can distinguish the physical interfaces to support the concepts of “inside” and “outside”. As this profile is specifically targeted at packet filters operating at the network and transport layers, it is assumed to have visibility into the headers of each of the protocols, which supply it with the “attributes” upon which access control decisions can be based. Using the TCP/IP protocol stack as an example, this would include such attributes as the source and destination IP address, source and destination port, and in some cases the presence or absence of certain flags in the headers (e.g., the ACK bit in TCP packets, presence of IP options). The only humans that directly interact with the firewall are administrators using a directly-attached console.

434 There is no authentication performed on the subjects (which are external to the firewall anyway), and the identification is provided “by default” since network addresses/transport service port identifiers are usually assigned outside of the scope of the firewall; e.g., IP addresses. No “user to subject binding” is maintained by the firewall, and it is left to the developer/ST author to determine what comprises the subject/object identity (that is, what the security relevant attributes of the subjects and objects are). This minimally comprises the network-layer address (e.g., IP

address), port, and location (e.g., physical interface, corresponding to “inside” and “outside”) of the subject/object. Given the address, port, location, and the direction of the packet (and in some cases certain other information, such as whether the ACK bit in the TCP header is set) most of the access control decisions that need to be made can be made.

Annex A

Rationale for CS1 Protection Profile

A.1 Introduction

435 This rationale material is the primary evaluation evidence and is included as an
example of how such rationale might be presented.

436 Rationale would not normally be included in the published profile but should be
made available to profile users by the registration authorities as required.

437 As an aid to evaluation, it is divided into sections which parallel the APE assurance
class. Readers and potential evaluators of this PP are invited to comment upon the
presentation, utility, and completeness of this material.

A.2 CS1 Security objectives

438 The CC requires that the PP security objectives are properly categorised as applied
to the TOE or its security environment, are useful and meaningful objectives, and
can be shown to cover all of the threats and policies identified.

439 No specific evidence is offered in support of any claims of utility of the stated
security objectives, the rationale aims to demonstrate that the objectives identified
provide a complete coverage of the threats and policies.

A.2.1 Threats to be addressed by the TOE

440 This section demonstrates that a TOE (in its environment) which meets all of the
stated security objectives will effectively counter all of the identified threats.

T.ACCESS An unauthorised person may gain logical access to the TOE.

441 O.LOGICAL reflects T.ACCESS directly.

442 O.RECORD leads to capture of a record of events which TOE management might
consider suspicious and indicative of possible attempted intrusions.

443 O.FLAW controls flaws in the TOE which might permit intrusion.

444 O.CONTROL ensures that the management capabilities exist to permit observation
and control of potential intrusion attempts.

445 O.INSTALL (Environment) asserts that the management support can and does
control intrusion.

- 446 O.PHYSICAL (Environment) asserts that potential intruders cannot gain access through direct assault on the machine.
- 447 O.CREDEN (Environment) asserts that intruders do not have access to stolen, forged, or otherwise improperly obtained authentication tokens.
- 448 O.CONN (Environment) asserts that intrusion emanating from uncontrolled network sources is not possible.
- T.AUTHOR** A user may gain access to resources for which no access rights have been granted.
- 449 O.ACCESS reflects T.AUTHOR directly.
- 450 O.RECORD ensures that the TOE collects data necessary to detect apparent penetration attempts by legitimate users.
- 451 O.ACCOUNT ensures that any apparent penetration attempts can be traced to the offending user.
- 452 O.BYPASS ensures that the functions and facilities offered to legitimate users by the TOE cannot be misused contrary to the security policy.
- 453 O.FLAW ensures that the TOE contains no residual flaws which could be exploited by a user.
- 454 O.CONTROL asserts that the TOE management possesses the necessary management tools to ensure that the TOE enforces the security policy.
- 455 O.INSTALL (Environment) asserts that the management support will control users adequately.
- 456 O.CREDEN (Environment) asserts that users do not have access to stolen, forged, or otherwise improperly obtained authentication tokens.
- T.TRACE** Security relevant events may not be recorded or may not be traceable to the user associated with the event.
- 457 O.ACCESS ensures that any record of attempted penetration cannot be deleted or modified to cover up the attempt.
- 458 O.RECORD ensures that the TOE can collect the information necessary to alert the TOE management to possible attempted penetration.
- 459 O.ACCOUNT ensures that, in the event of an attempted insider attack, the correct miscreant can be identified.
- 460 O.BYPASS ensures that it is not possible to avoid the creation of the necessary evidence of intrusion.

- 461 O.FLAW ensures that undiscovered flaws cannot be exploited to cover an intruder's tracks.
- 462 O.CONTROL ensures that the TOE management possesses the necessary facilities to identify miscreants.
- 463 O.INSTALL (Environment) asserts that the management support is available to enforce proper record keeping.
- 464 O.CREDEN (Environment) asserts that stolen, forged, or otherwise improperly obtained authentication tokens are not used to impersonate legitimate users.
- 465 O.CONN (Environment) asserts that intrusion emanating from uncontrolled network sources is controlled.

T.FLAW Security failures may occur because of flaws in the TOE.

- 466 O.FLAW reduces to an acceptable level the probability that such flaws exist.

A.2.2 Threats to be addressed by the operating environment

- 467 This section demonstrates that the threats to be countered by the security environment of the TOE map to the security objectives identified for the environment.

T.PHYSICAL Security-critical parts of the TOE may be subjected to physical attack which may compromise security.

- 468 O.INSTALL (Environment) asserts that the TOE management will continue to enforce the necessary physical controls.

- 469 O.PHYSICAL (Environment) asserts that the TOE management will put the necessary physical controls in place.

T.OPERATE Security failures may occur because of improper administration and operation of the TOE.

- 470 O.INSTALL (Environment) asserts that TOE management accept the responsibility for countering this threat.

- 471 O.CREDEN (Environment) asserts that TOE users accept the responsibility for countering this threat.

- 472 O.CONN (Environment) asserts that the TOE management covers all IT resources which could impact upon the TOE security.

A.2.3 Satisfaction of policies

P.KNOWN Legitimate users of the TOE must be identified before TOE access can be granted.

473 O.LOGICAL ensures that unknown persons can be denied the relevant access.

P.TRUST Legitimate users of the system, once granted access to information, are trusted to manage the subsequent control of that information.

474 O.ACCESS ensures that the TOE can enforce such a discretionary policy.

P.ACCESS Access rights to specific data objects are determined by attributes assigned to that object, the identity of the user, and attributes associated with that user.

475 O.ACCESS ensures that the TOE can enforce such a discretionary policy.

P.ACCOUNT Users must be held accountable for their important security actions.

476 O.ACCOUNT ensures that the TOE can enforce such an accountability policy.

A.2.4 Completeness of objectives

477 Table A.1 below shows the mapping of each objective to the threats and policies.

Objective	Threats	Policies
O.LOGICAL	T.ACCESS	P.KNOWN
O.ACCESS	T.AUTHOR T.TRACE	P.TRUST P.ACCESS
O.RECORD	T.ACCESS T.AUTHOR T.TRACE	
O.ACCOUNT	T.AUTHOR T.TRACE	P.ACCOUNT
O.BYPASS	T.AUTHOR T.TRACE	
O.FLAW	T.ACCESS T.AUTHOR T.TRACE T.FLAW	
O.CONTROL	T.ACCESS T.AUTHOR T.TRACE	

Table A.1 - Mapping of security objectives to threats and policies

Objective	Threats	Policies
O.INSTALL (E)	T.ACCESS T.AUTHOR T.TRACE T.PHYSICAL T.OPERATE	
O.PHYSICAL (E)	T.ACCESS T.PHYSICAL	
O.CREDEN (E)	T.ACCESS T.AUTHOR T.TRACE T.OPERATE	
O.CONN (E)	T.ACCESS T.TRACE T.OPERATE	

Table A.1 - Mapping of security objectives to threats and policies

478 Table A.1 indicates that all objectives contribute to the ability of the TOE to counter
a threat and/or satisfy a policy and that all threats and policies have been addressed.
Thus there are no unnecessary objectives.

479 No evaluation evidence is offered specifically in support of the claim that the
objectives are sufficient to satisfy fully all threats and policies. Evaluators should
consider the merits of the discussion of each threat and policy.

A.3 CS1 Functional requirements rationale

480 This section lists the individual components included in the profile and contains the
full wording of the elements of those components.

481 Refinements of the element wording are indicated by italicising the refined text and,
where necessary, explaining the refinement in following paragraphs.

482 Explanations of refinements and the justifications for the inclusion of the
component are distinguished by the use of distinct fonts.

FIA_UID.1 User Identification

483 **FIA_UID.1.1** The TSF shall identify each user before performing any actions
requested by the user.

484 This requirement does not reconstruct the FC/TCSEC identification requirements
precisely. FC/CS1 includes the conditional ‘shall be able to ..by providing the
capability to identify each individual user’ implying that uniqueness is an option.

485 In the context of identification, the FC & the CC use the term ‘user’ to cover both
those authenticated (& hence identified) by the TOE, and the community of
individuals with the authority to use the TOE. The TCSEC uses the term ‘individual
ADP system user’ for the latter.

486 The loss of the uniqueness is not significant - as it is not mandated, then it must be
supplied as part of the administrative responsibilities. The TOE supports but does
not enforce unique user-ids, but the administrators can.

487 This component is a prerequisite to the entry objective O.LOGICAL, the access
control objective O.ACCESS, and the accountability objective O.ACCOUNT.

FIA_UAU.1 Basic User Authentication

488 **FIA_UAU.1.1** The TSF shall authenticate any user’s claimed identity prior to
performing any functions for the user.

489 FC/CS1 has no explicit authentication requirement, it is implicit in fragment I&A-
1.1.2 though this can be read otherwise.

490 For this profile, I&A-1.1.2 is interpreted to read ‘The TCB shall authenticate the
user’s identity.’ & ‘The TCB shall use a protected mechanism...’.

491 The example reference to passwords in FC/CS1 I&A-1.2 is included as a note.

492 This component is a prerequisite to the entry objective O.LOGICAL, the access
control objective O.ACCESS, and the accountability objective O.ACCOUNT.

FIA_ATD.1 User Attribute Definition

493 **FIA_ATD.1.1** The TSF shall provide, for each user, a set of security attributes
necessary to enforce the TSP.

494 This requirement permits, but does not enforce, uniqueness. The granularity of the
user attribute definitions is determined by the TOE administration. This
requirement does not comment on whether user attributes are shared or unique,
merely that each user should have the necessary attributes.

495 This component is a prerequisite to the entry objective O.LOGICAL, the access
control objective O.ACCESS, and the accountability objective O.ACCOUNT.

FIA_ATA.1 User Attribute Administration

496 **FIA_ATA.1.1** The TSF shall provide the ability to initialise user attributes with
provided default values.

497 This will reduce the chance of selection of unsuitable user attributes by providing
acceptable defaults. The higher level components which require specific checks on
the default attributes are not included. Initial user attributes must meet the implicit
requirement that the policy be enforced.

498 This component is a prerequisite to the entry objective O.LOGICAL, the access control objective O.ACCESS, and the accountability objective O.ACCOUNT.

FIA_ADP.2 Extended User Authentication Data Protection

499 **FIA_ADP.2.1** The TSF shall protect from unauthorised observation, modification, and destruction the raw form of authentication data at all times while it resides in the TOE.

500 Authentication depends upon the veracity, and possibly the secrecy, of authentication data. Thus unless adequate controls are imposed, the authentication requirements cannot be met.

501 Extended protection is called up to meet the I&A-1.2 requirement for a 'protected mechanism' to include such controls as password file encryption and non display of passwords on entry.

502 This component is a prerequisite to the entry objective O.LOGICAL, the access control objective O.ACCESS, and the accountability objective O.ACCOUNT.

FAU_GEN.1 Audit Data Generation

503 **FAU_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions.
- b) All auditable events for the *basic* level of audit, as defined in all functional components included in CC/CS1:
 - 1) [FIA_UID] All attempts to use the user identification mechanism, including the user identity provided. *The origin of request shall be included in the audit record.*
 - 2) [FIA_UAU] Any use of the authentication mechanism. *The origin of request shall be included in the audit record.*
 - 3) [FIA_ATA] All attempted uses of the user attribute administration function including Identification of the user attributes that have been modified.
 - 4) [FIA_ADP] All requests to access user authentication data.
 - 5) [FAU_PRO] Any attempt to read, modify, or destroy the audit trail.
 - 6) [FAU_MGT.1] Any attempt to perform an operation on the audit trail.
 - 7) [FAU_SEL] All modifications to the audit configuration that occur while the audit collection functions are operating.
 - 8) [FDP_ACF] All *requests* to perform an operation on an object covered by the *Discretionary Access Control Policy including*

introduction of objects into a user's address space, and deletion of objects.

- 9) [FDP_ACI] Any changes or overriding of the default object attributes including which default object attributes have been changed or overridden.
- 10) [FDP_SAM] All attempts to modify security attributes including the identity of the target of the modification attempt and the new values of the modified security attributes
- 11) [FPT_AMT] Execution of the tests of the underlying machine and the results of the tests.
- 12) [FPT_TSA] Use of a security relevant administrative function.

c) *[assignment: other auditable events]*

504 Refinement is used to insert operations which permit the ST writer to add further audit events as required.

505 **FAU_GEN.1.2** The TSF shall record within each audit record at least the following information:

- a) date and time of event, type of event, subject identity, and *outcome (i.e. success or failure)* of the event.
- b) For each audit record type, based on the auditable event definitions of the functional components included in CC/CS1, *[assignment: other information relevant to the audited event]*.

506 The selection [success,failure] is refined into outcome in the interests of clarity.

507 This component defines the audit record type and the contents. The ST record contents must be completed by the ST author.

508 This component is primarily directed against the accountability objective O.ACCOUNT.

FAU_GEN.2 User Identity Generation

509 **FAU_GEN.2.1** The TSF shall be able to associate any auditable events with the identity of the user responsible for the events.

510 FAU_GEN.1 requires traceability to the subject id only, this component adds to that by requiring that the user id that owns the subject be determined also.

511 This component is primarily directed against the accountability objective O.ACCOUNT.

FAU_STG.1 Security Audit Event Storage

512 **FAU_STG.1.1** The TSF shall store generated audit records in a permanent audit trail.

513 Called up by audit protection, necessary to ensure that the audit record persists beyond periods of TOE operation.

514 This component is primarily directed against the accountability objective O.ACCOUNT.

FAU_PRO.1 Security Audit Trail Protection

515 **FAU_PRO.1.1** The TSF shall restrict access to the audit trail to the authorised administrator.

516 This requirement is necessary to ensure that intruders and other threat agents cannot subvert the audit trail in order to remove traces of their activities.

517 This component is primarily directed against the accountability objective O.ACCOUNT.

FAU_MGT.1 Audit Trail Management

518 **FAU_MGT.1.1** The TSF shall provide the authorised administrator with the ability to *create, delete, and empty* the audit trail.

519 These are the most basic administration features (FC/CS1 is silent on the specifics). The management requirements might be supplemented by audit review requirements in the ST.

520 This component is primarily directed against the accountability objective O.ACCOUNT.

FAU_SEL.1 Selective Audit

521 **FAU_SEL.1.1** The TSF shall be able to include or exclude auditable events from the set of audited events based on *one or more of* the following attributes:

- a) User identity
- b) Object attributes

522 This meets the FC/AD-1-4b requirement with ‘individual identity’ replaced by ‘user identity’ as uniqueness of the individual is not enforced. In practice, extended selection criteria such as subject identity and event type and outcome could be usefully included.

523 This component is primarily directed against the accountability objective O.ACCOUNT.

FAU_SEL.2 Runtime Selection Mode

524 **FAU_SEL.2.1** The TSF shall provide the authorised administrator with the capability to select, at any time during the operation of the TOE, which events are to be audited.

525 Required to make the audit capability more responsive to suspected intrusion or other undesirable activity.

526 This component is primarily directed against the accountability objective O.ACCOUNT.

FPT_TSA.1 Basic Security Administration

527 **FPT_TSA.1.1** The TSF shall distinguish security-relevant administrative functions from other functions.

528 **FPT_TSA.1.2** The TSF's set of security-relevant administrative functions shall include all functions necessary to install, configure, and manage the TSF; minimally, this set shall include:[assignment: list of administrative services to be minimally supplied]

529 **FPT_TSA.1.3** The TSF shall restrict the ability to perform security-relevant administrative functions to specifically authorised users.

530 **FPT_TSA.1.4** The TSF shall be capable of distinguishing the set of users authorised for administrative functions from the set of all users of the TOE.

531 Adequate administration capability is a general requirement which contributes to the meeting of all security objectives.

FPT_TSU.1 Administrative Safe Use

532 **FPT_TSU.1.1** The TSF shall enforce checks for valid input values for security relevant administrative functions as described in the Administrative Guidance.

533 This general administration requirements contributes to all objectives by reducing the probability of operator errors leading to insecure configuration.

FDP_ACC.1 Subset Object Access Control

534 **FDP_ACC.1.1** The TOE shall enforce the *Discretionary Access Control Policy* on:

- a) *users*
- b) *subjects acting upon behalf of users*
- c) *other named subjects*
- d) *named objects which contain user data*
- e) *[assignment: operations among subject and objects covered by the access rules].*

535 The CC requires the particular policies enforced to be named. The primary access control policy is named 'Discretionary Access Control Policy' in line with community expectations and conventions - though the term DAC is not employed in the FC/CS1 requirements.

536 The refinements expand to the defining characteristics of DAC subjects and objects. The operations cannot be determined by the PP, these have to be defined in the ST.

537 This component is primarily directed against the access control objective O.ACCESS.

FDP_ACF.1 Single Security Attribute Access Control

538 **FDP_ACF.1.1** The TSF shall enforce *the Discretionary Access Control Policy* on objects based on *the following subject attributes*:

- a) *user identity: user identity from user attributes*
- b) *group list: zero or more group identities from user attributes*
- c) *[assignment: subject type: nature of the subject]*

539 **FDP_ACF.1.1** The TSF shall enforce *the Discretionary Access Control Policy* on objects based on the following object attributes:

- a) *access control list: a list of groups and users with, for each group or user, a list of the specific operations permitted on the object by each group or user;*
- b) *[assignment: object type: the nature of the controlled object].*

540 **FDP_ACF.1.2** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- a) *If the subject user identity or any member of the subject group list is mentioned in the access control list of the object, then the subject shall be granted the access permissions mentioned in the access control list.*
- b) *If neither the subject user identity nor any member of the subject group list is mentioned in the access control list of the object, then access shall be granted by application of the [assignment: default access rules].*
- c) *If consulting the access control list returns a non-unique result, then the ambiguity shall be resolved by application of [assignment: rules for the consultation of access control lists].*

541 *If different rules apply to different subjects and objects, the totality of these rules shall be shown to support the overall policy.*

542 This component expands the DAC attributes mediation rules to the extent that is sensible without constraining the implementation.

- 543 User attributes are constrained to the user/group notion with multiple groups supported. An assignment is left should additional subject attributes required. This will permit further control by requiring that independent restrictions may apply to certain subject (e.g. application) types.
- 544 Object attributes are limited to access control lists with an open assignment that permits the object type to be factored into the access mediation.
- 545 The basic access list mediation rules are defined. These do not cover the rules for resolution of conflicts or global access permissions. Assignments are provided for the ST write to define these.
- 546 A further refinement opportunity is added to permit the subject and object types to be factored in. The FC requirement is repeated to achieve this.
- 547 The FC requirement is also factored into the audit requirement.
- 548 This component is primarily directed against the access control objective O.ACCESS.

FDP_ACI.1 Static Attribute Initialisation

- 549 **FDP_ACI.1.1** The TSF shall enforce *the Default Attributes Policy* to provide *valid user supplied* or default values for the object security attributes that are used to enforce *the policy*.
- 550 **FDP_ACI.1.2** The TSF shall allow the specification of alternate initial values to override the default values when the object is created.
- 551 A policy is required to determine the initial values that objects take upon creation. The details are left open as to whether the user is always consulted, or whether the TOE can supply defaults which might be selected by the user.
- 552 This component is primarily directed against the access control objective O.ACCESS.

FDP_SAM.2 User Attribute Modification

- 553 **FDP_SAM.2.1** The TSF shall enforce *the following access rules* to provide authorised users with the ability to modify *object attributes*.
- a) *Access permission to an object by users not already possessing access permission shall be assigned only by authorised users.*
 - b) *[assignment: additional rules for the modification of object attributes]*
- These rules shall allow authorised users to specify and control sharing of objects by named individuals or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights.*

If different rules of assignment and modification of access control attributes apply to different subjects and/or objects, the totality of these rules shall be shown to support the defined policy.

554 No specific attribute modification rules are defined, it is the responsibility to create these in line with the overall DAC policy objectives. The specific FC requirements are repeated by way of a refinement (other than granularity which is covered under ACF.1).

555 Some further interpretation is required here, in particular it is not clear what the significance of 'controls to limit the propagation of access rights' is within the framework of a DAC policy. The relevant TCSEC/C2 interpretations should be consulted.

556 This component is primarily directed against the access control objective O.ACCESS.

FDP_RIP.1 Subset Residual Information Protection

557 **FDP_RIP.1.1** The TSF shall ensure that upon the allocation of a resource to *objects which contain user data* any previous information content (*including encrypted representations*) is unavailable.

558 The assignment *objects which contain user data* is used because the FC/CS1 is non-specific.

559 The refinement (*including encrypted representations*) brings in a specific requirement from FC/CS1 AC-1-4d but is not further elaborated.

560 This component has been included in answer to objective O.ACCESS. It ensures that a particular class of implementation shortcoming does not undermine the access control policy and should also be traced to O.FLAW.

FPT_SEP.1 TSF Domain Separation

561 **FPT_SEP.1.1** The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

562 Element FPT_SEP.1.1 does not, itself, need refinement. However, the FC P-1 component adds further implementation constraints which are added as the refinements below. They are translated into CC terminology with the wording minimally clarified.

- a) *The transfers between TSF and non-TSF domains shall be controlled such that arbitrary entry to or return from the TSF is not possible.*
- b) *User or application parameters passed to the TSF by reference shall be validated with respect to the TSF address space, and those passed by value shall be validated with respect to the values expected by the TSF.*

- c) *The permissions of objects (and/or to non-TSF data) passed as parameters to the TSF shall be validated with respect to the permissions required by the TSF.*
- d) *References to TSF objects used by TSF isolation functions shall be mediated by the TSF.*
- e) *The TSF domain shall include all user and object attributes.*

563 Some of these requirements are specific implementation constraints rather than security requirements. Future issues of this profile should consider whether they are more appropriate as application notes.

564 Refinement (d) makes explicit a requirement that is implicit in the CC to meet the specific FC/CS1 requirement. The CC notes should be consulted on the scope of the term TSF data which is implicitly protected by this requirement.

565 **FPT_SEP.1.2** The TSF shall enforce separation between the security domains of subjects in the TSC.

566 Element FPT_SEP.1.2 is not required by FC/CS1.

567 This component is necessary in order to be able to reason about the access control policy enforcement objective O.ACCESS. The corresponding control objective is O.BYPASS.

FPT_RVM.1 Non-Bypassability of the TSP

568 **FPT_RVM.1.1** The TSF shall ensure that the TSP enforcement functions are invoked and succeed before any security related operation is allowed to proceed.

- a) *The TSF shall mediate all references to subjects, objects, resources, and TSF functions.*
- b) *The mediation shall ensure that all subject object references are directed to the Discretionary Access Control Policy functions.*
- c) *The mediation shall ensure that all resource references are directed to the residual information protection functions.*
- d) *References issued by privileged subjects shall be mediated in accordance with the policy attributes defined for those subjects.*

569 FC/CS1 provides more detail on the reference mediation requirements. These have been rephrased to use the CC/CS1 terminology and repeated as refinements.

570 This component is necessary in order to be able to reason about the access control policy enforcement objective O.ACCESS. The corresponding control objective is O.BYPASS.

FPT_AMT.1 Abstract Machine Testing

571 **FPT.AMT.1.1** The TSF shall provide the authorised administrator with the
capability to validate the correct operation of the security-relevant functions
provided by the *hardware and firmware upon which the TOE operates*.

572 As the TOE is an operating system, the words ‘TSF’s underlying abstract machine’
have been replaced by a reference to the actual hardware ‘hardware and firmware
upon which the TOE operates’. This then reconstructs the FC/CS1 requirement.

573 This component has been included primarily in answer to O.FLAW, hardware
failure is an (albeit temporary) implementation flaw.

A.4 CS1 Functional requirements dependencies

574 Functional components possess dependencies which are stated requirements for the
CS1 to include further components in support of the primary requirements.

575 To meet the evaluation requirements, it is necessary for all dependencies to be
satisfied. Table A.2 below demonstrates how the dependencies of each included
component have been satisfied.

576 All the components of the CC/CS1 profile are listed with a numeric reference
(Ref1). The dependencies of each component are listed alongside that component
with the reference of that component within the table (Ref2).

577 The table demonstrates that CS1 has no internally unsatisfied dependencies

Ref1	Component	Dependencies	Ref2
1	FIA_UID.1	FIA_ATD.1	3
2	FIA_UAU.1	FIA_UID.1	1
3	FIA_ATD.1	ADV_FSP.1	EAL3
4	FIA_ATA.1	FIA_ATD.1 FPT_TSA.1	3 13
5	FIA_ADP.1	FIA_UAU.1	2
6	FAU_GEN.1	FIA_UID.1	1
7	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	6 1
8	FAU_STG.1	FAU_GEN.1	6
9	FAU_PRO.1	FAU_STG.1 FPT_TSA.1	8 13
10	FAU_MGT.1	FAU_STG.1	8
11	FAU_SEL.1	FAU_GEN.1	6
12	FAU_SEL.2	FAU_SEL.1 FPT_TSA.1	11 13

Table A.2 - Functional component dependency analysis

13	FPT_TSA.1	FIA_UID.1 FIA_ATD.1 FIA_ATA.1 AGD_ADM.1	1 3 4 EAL3
14	FPT_TSU.1	FPT_TSA.1 AGD_ADM.1	13 EAL3
15	FDP_ACC.1	FDP_ACF.1	16
16	FDP_ACF.1	FDP_ACC.1	15
17	FDP_ACI.1	FDP_ACF.1 FPT_TSU.1	16 14
18	FDP_SAM.2	FPT_TSA.1 FDP_ACC.1	13 15
19	FDP_RIP.1	-	-
20	FPT_SEP.1	-	-
21	FPT_RVM.1	-	-
22	FPT_AMT.1	-	-

Table A.2 - Functional component dependency analysis

A.5 CS1 Assurance requirements rationale

578 The CC does not attempt to reconstruct the assurance levels and assurance elements of the classes of the source criteria. The source criteria were developed at different times and with some differences with respect to assurance philosophy. As such, there is no simple mapping between the assurance packages and levels of the source criteria.

579 The CC EALs are intended to provide a uniform assurance scale which, though the points on it do not match previous criteria exactly, provides a reasonable equivalency in terms of overall assurance gained.

580 EAL3 is selected for CC/CS1 as it is intended to correspond on the CC EAL assurance scale to the assurance content of the FC/CS1 and TCSEC/C2 profiles.

581 EAL3 requires a some security specific engineering and developmental controls which equate to 'good commercial practice'. The balance of costs and benefits of EAL3 is appropriate for the security functions offered and the perceived market for CS1 class products.

A.6 Mapping to FC/CS1 requirements

A.6.1 Mapping to FC/CS1 functional requirements

582 CC CS1 is intended to model FC/CS1 requirements insofar as this is feasible using the CC components. The table below shows where each of the individual FC/CS1 functional requirements are represented in the CC/CS1.

583 The FC components are presented at a higher level of aggregation than the CC components. FC components have been dissected and the references have been extended so as to refer to what corresponds to elements in the CC.

584 Table A.3 below shows where each FC/CS1 requirements fragment has been addressed in CC/CS1 and comments where the match is inexact or FC specific refinements have been made.

FC Reference	FC Functional Element	CC Correspondence
I&A-1.1.a	The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate.	FIA_UID.1 calls up the identification requirement. FC/CS1 does not call up authentication as a distinct requirement, CC/CS1 adds this explicitly with FIA_UAU.1.
I&A-1.1.b	The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual user.	FIA_UID.1 supports, but does not enforce, unique user-ids. The capability exists but the administrators must enforce it.
I&A-1.1.c	The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.	FAU_GEN.2 is the same though expression is inverted.
I&A-1.2	The TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity.	Not clear what 'protected mechanism' means. If interpreted as there shall be an authentication mechanism, and that authentication is part of the TSF, then FPT_SEP.1 requires protection of the authentication mechanism. If this clause is a requirement for authentication, then FIA_UAU.1 covers it. The password example is noted here.
I&A-1.3	The TCB shall protect authentication data so that it cannot be used by any unauthorized user.	FIA_ADP.1 matches this with a specific refinement of 'used'
AD-1-1.a1	The TCB shall be able to create,	FAU_GEN.1 addresses this area in general.
AD-1-1.a2 maintain,	FAU_MGT.1 interprets this as specific management requirements.
AD-1-1.a3 and protect from modification or unauthorized access or destruction an audit trail	Protection aspects not explicitly addressed, inference from the restriction requirement of FAU.PRO. As TSF data, the audit trail shall be protected by virtue of FPT.SEP.1

Table A.3 - Mapping to FC/CS1 functional requirements

FC Reference	FC Functional Element	CC Correspondence
AD_1-1.a4 of accesses to the objects it protects.	This is an implicit requirement to audit object accesses. There is an explicit requirement for auditable events later. Addressed by FAU.GEN.1 elaboration.
AD-1-1.b	The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data.	FAU.PRO.1 matches this requirement where 'those who are authorized' becomes 'authorised administrator'
AD-1-2.a	The TCB shall be able to record the following types of events: - use of the identification and authentication mechanisms;	FAU_GEN.1 with the... specific audit requirements from FIA_UAU and FIA_UID.
AD-1-2.b	The TCB shall be able to record the following types of events: - introduction of objects into a user's address space (e.g., file open, program initiation), and deletion of objects;	FAU_GEN.1 with the specifics from FDP_ACF. As CC/CS1 is not specific about the objects and operations, the FC requirement and examples are added as a specific refinement.
AD-1-2.c	The TCB shall be able to record the following types of events: - actions taken by computer operators and system administrators and/or system security officers.	FAU_GEN.1 with a refinement against FPT_TSA of an operation for this audit requirement.
AD-1-3.a	For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event.	FAU_GEN.1.2a is essentially the same requirement.
AD-1-3.b	For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record.	Added as a refinement on the specific audit requirements for FIA_UID & FIA_UAU.
AD-1-3.c	For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name and policy attributes of the object (e.g., object security level).	The specific requirement is included in the relevant FDP_ACF audit requirements. The example 'object security level' is not added as a refinement as it is possibly misleading for DAC and not in the list of object attributes.
AD-1-4a	The system administrator shall be able to selectively audit	FAU_SEL.1 call up the basic functionality, FAU_SEL.2 requires the administration features to support it.

Table A.3 - Mapping to FC/CS1 functional requirements

FC Reference	FC Functional Element	CC Correspondence
AD-1-4bthe actions of one or more users based on individual identity and/or object policy attributes (e.g., object security level).	FAU_SEL.1 identifies specific attributes. The exemplary 'object security level' has not been refined in though it has more of a MAC than DAC flavour.
AC-1-1.a	The TCB shall define and protect access control attributes for subjects and objects.	Covered implicitly under FPT_SEP.1 but, to emphasise the point, this requirement is added as a specific refinement FPT_SEP.1d.
AC-1-1.b	Subject attributes shall include named individuals or defined groups or both.	Covered as a refinement of FDP_ACF.1.1.
AC-1-1.c	Object attributes shall include defined access rights (e.g., read, write, execute) that can be assigned to subject attributes.	Covered as a refinement of FDP_ACF.1.1.
AC-1-2.a	The TCB shall define and enforce rules for assignment and modification of access control attributes for subjects and objects.	Covered as FDP_SAM.2.
AC-1-2.b	The effect of these rules shall be that access permission to an object by users not already possessing access permission is assigned only by authorized users.	Covered as a refinement of FDP_SAM.2.
AC-1-2.c	These rules shall allow authorized users to specify and control sharing of objects by named individuals or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights.	Covered as a refinement of FDP_SAM.2, the specific rules are left as an open assignment. The requirement to 'limit propagation of access rights' requires more explanation as it seems counter to the DAC policy.
AC-1-2.d	These controls shall be capable of including or excluding access to the granularity of a single user.	Covered as a refinement of FDP_ACF.1.
AC-1-2.e	If different rules of assignment and modification of access control attributes apply to different subjects and/or objects, the totality of these rules shall be shown to support the defined policy.	Covered as a refinement of FDP_SAM.2, the specific rules are left as an open assignment.
AC-1-3.a	The TCB shall define and enforce authorization rules for the mediation of subject references to objects.	See FDP_ACF.1.2
AC-1-3.b	These rules shall be based on the access control attributes of subjects and objects.	... which elaborates some of them, but defers definition of resolution of conflicts within ACLs.

Table A.3 - Mapping to FC/CS1 functional requirements

FC Reference	FC Functional Element	CC Correspondence
AC-1-3.c	These rules shall, either by explicit user action or by default, provide that objects are protected from unauthorized access.	Covered as FDP_ACF.1.2.
AC-1-3.d	The scope of the authorization rules shall include a defined subset of the product's subjects and objects and associated access control attributes.	Covered as FDP_ACC.1.
AC-1-3.e	The coverage of authorization rules shall specify the types of objects and subjects to which these rules apply.	Covered as FDP_ACC.1 which requires the subjects and object covered to be identified, and FDP_ACF.1.1 which brings the types of the subjects and objects into the access mediation.
AC-1-3.f	If different rules apply to different subjects and objects, the totality of these rules shall be shown to support the defined policy.	Added explicitly as a refinement on FDP_ACF.1.2.
AC-1-4.a	The TCB shall control the creation and destruction of subjects and objects.	Implicit in the inclusion of FDP_RIP and the access control rules.
AC-1-4.b	These controls shall include object reuse.	FDP_RIP deals with these issues though the correspondence is not exact.
AC-1-4.c	That is, all authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects;	FDP_RIP.1 with refinements for creation/deletion 'don't care'
AC-1-4.d	information, including encrypted representations of information, produced by a prior subjects' actions shall be unavailable to any subject that obtains access to an object that has been released back to the system.	FDP_RIP.1 with refinement for encrypted representation
RM-1-1.a	The TCB shall mediate all references to subjects, objects, resources, and services (e.g., TCB functions) described in the TCB specifications.	FPT_RVM.1 is the CC reference monitor requirement but is terse. The FC/CS1 specifics are added as a refinement of FPT_RVM. The wording is amended to be compatible with the CC terminology and approach.
RM-1-1.b	The mediation shall ensure that all references are directed to the appropriate security-policy functions.	These FC/CS1 specifics are added as a refinement of FPT_RVM.

Table A.3 - Mapping to FC/CS1 functional requirements

FC Reference	FC Functional Element	CC Correspondence
RM-1-2	Reference mediation shall include references to the defined subset of subjects, objects, and resources protected under the TCB security policy, and to their policy attributes (e.g., access rights, security and/or integrity levels, role identifiers).	These FC/CS1 specifics are added as a refinement of FPT_RVM.
RM-1-3	References issued by privileged subjects shall be mediated in accordance with the policy attributes defined for those subjects.	These FC/CS1 specifics are added as a refinement of FPT_RVM.
P-1.a	The TCB shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modification of its code and data structures).	FPT_SEP.1 reproduces the intent of this requirement in CC vocabulary. Also brings in an additional requirement SEP.1.2 concerning separation of untrusted subjects from each other - this is not required by FC/CS1.
P-1.b-1.(1)	<p>The protection of the TCB shall provide TCB isolation and noncircumventability of TCB isolation functions as follows:</p> <p>TCB Isolation requires that (1) the address spaces of the TCB and those of unprivileged subjects are separated such that users, or unprivileged subjects operating on their behalf, cannot read or modify TCB data structures or code</p>	<p>This is further elaboration of the fundamental requirement P-1a and is addressed by FPT_SEP.1.</p> <p>Essentially, this is gratuitous explanation and does not need to be perpetuated.</p>
P-1.b-1.(2)	<p>The protection of the TCB shall provide TCB isolation and noncircumventability of TCB isolation functions as follows:</p> <p>TCB Isolation requires that, -- (2) the transfers between TCB and non-TCB domains are controlled such that arbitrary entry to or return from the TCB are not possible; and</p>	<p>This looks like a requirement for controlled gateways between domains.</p> <p>The CC avoids unnecessary implementation constraints, this material must therefore be added explicitly as an implementation refinement.</p>
P-1.b-1.(3)	<p>The protection of the TCB shall provide TCB isolation and noncircumventability of TCB isolation functions as follows:</p> <p>TCB Isolation requires that, -- (3) the user or application parameters passed to the TCB by addresses are validated with respect to the TCB address space, and those passed by value are validated with respect to the values expected by the TCB.</p>	The CC avoids unnecessary implementation constraints, this material must therefore be added explicitly as an implementation refinement.

Table A.3 - Mapping to FC/CS1 functional requirements

FC Reference	FC Functional Element	CC Correspondence
P-1.b-2	Noncircumventability of TCB isolation functions requires that the permission to objects (and/or to non-TCB data) passed as parameters to the TCB are validated with respect to the permissions required by the TCB, and references to TCB objects implementing TCB isolation functions are mediated by the TCB.	The CC avoids unnecessary implementation constraints, this material must therefore be added explicitly as an implementation refinement.
SC-1	Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.	FPT.AMT.1 provides basic requirement refined for hardware testing.

Table A.3 - Mapping to FC/CS1 functional requirements

A.6.2 Mapping to FC/CS1 assurance requirements

- 585 CC/CS1 does not reconstruct the precise assurance requirement of FC/CS1 and TCSEC/CS1, rather it aims to achieve the same effective assurance using the CC defined EALs.
- 586 Table A.4 below dissects the FC/CS1 assurance requirements and discussed, for each requirement, the extent to which it is covered by the selected CC assurance level.
- 587 This analysis has not covered the reverse traceability in any depth. Not all CC requirements that exceed the FC/CS1 requirements are identified here.

FC Reference	FC Assurance Element	CC Correspondence Notes
PD-1.a	The developer shall interpret the functional requirements of the protection profile within the product TCB.	Covered in the requirements for the ST, the ST is intended to be the precise interpretation of the PP for the specific TOE.
PD-1.b.(1)	For each functional requirement, the developer shall: (1) identify the TCB elements and their TCB interfaces (if any) that implement that requirement;	Covered as ADV.RCR.1 requires that the security functions which define the TSF interface are traced to the PP requirements.

Table A.4 - Mapping to FC/CS1 assurance requirements

FC Reference	FC Assurance Element	CC Correspondence Notes
PD-1.b.(2)	For each functional requirement, the developer shall: -- (2) describe the operation of these TCB elements, and	Covered, ADV.RCR.1 requires the security functions to be traced to the requirements, ADV_FSP.1 requires that the interface and behaviour of the TSF be defined.
PD-1.b.(3)	For each functional requirement, the developer shall: -- (3) explain why the operation of these elements is consistent with the functional requirement.	Covered as ADV_RCR.1 though expressed differently.
ID-1.a	The developer shall identify the TCB elements (i.e., software, hardware/firmware code and data structures).	Partially covered only down to the high level design with sampling of lower levels where the evaluator requires them.
ID-1.b	Each element must be unambiguously identified by its name, type, release, and version number (if any).	Partially covered only, ACM_SCP.1 CM requirements imply this but leave the details to the developer.
IF-1.a	The developer shall describe all external (e.g., command, software, and I/O) administrative (i.e., privileged) and non-administrative interfaces to the TCB.	Covered under ADV_FSP.1 and the requirement to define the TSFI.
IF-1.b	The description shall include those components of the TCB that are implemented as hardware and/or firmware if their properties are visible at the TCB interface.	Covered implicitly in ADV_FSP.1 and the declared scope of the CC as including hardware and firmware where necessary.
IF-1.c	The developer shall identify all call conventions (e.g., parameter order, call sequence requirements) and exceptions signaled at the TCB interface.	Not an explicit requirement of ADV_FSP.1, implicit in the requirement to document the TSFI 'syntax and semantics'.
FT-1.a	The developer shall test the TCB interface to show that all claimed protection functions work as stated in the TCB interface description.	Covered by ATE_FUN.1, though the CC is rather more rigorous with respect to testing, both penetration testing and functional testing.
FT-1.b	The developer shall correct all flaws discovered by testing and shall retest the TCB until the protection functions are shown to work as claimed.	CC has no explicit requirements to correct flaws, this is implicit in the requirement that the tests should show a positive outcome. Penetration testing requires a disposition of vulnerabilities.

Table A.4 - Mapping to FC/CS1 assurance requirements

FC Reference	FC Assurance Element	CC Correspondence Notes
UG-1.a	The developer shall provide a User Guide which describes all protection services provided and enforced by the TCB.	Covered with more detail in AGD_USR.1
UG-1.b	The User Guide shall describe the interaction between these services and provide examples of their use.	Covered in AGD_USR.1 though the wording is different and somewhat more demanding.
UG-1.c	The User Guide may be in the form of a summary, chapter or manual.	Not covered in the CC, not a security requirement. AVA_MSU.1 requires usable guidance.
UG-1.d	The User Guide shall specifically describe user responsibilities.	Not covered explicitly in AGD_USR.1, equivalent wording is 'describe privileges...including warnings regarding their use'.
UG-1.e	These shall encompass any user responsibilities identified in the protection profile.	Not covered, specifically O.CREDEN is laid on the environment. AGD_ADM.1 requires that the environmental issues be addressed in the administration documentation. AGD_USR is not specific on these issues.
AG-1.a	The developer shall provide a Trusted Facility Manual intended for the product administrators that describes how to use the TCB security services (e.g., Access Control, System Entry, or Audit) to enforce a system security policy.	Covered differently in AGD_ADM.1.
AG-1.b	The Trusted Facility Manual shall include the procedures for securely configuring, starting, maintaining, and halting the TCB.	Covered differently in AGD_ADM.1.
AG-1.c	The Trusted Facility Manual shall explain how to analyze audit data generated by the TCB to identify and document user and administrator violations of this policy.	Covered differently in AGD_ADM.1.
AG-1.d	The Trusted Facility Manual shall explain the privileges and functions of administrators.	Covered differently in AGD_ADM.1.
AG-1.e	The Trusted Facility Manual shall describe the administrative interaction between security services.	Covered differently in AGD_ADM.1.
AG-1.f	The Trusted Facility Manual shall be distinct from User Guidance, and encompass any administrative responsibilities identified in security management.	Covered differently in AGD_ADM.1.

Table A.4 - Mapping to FC/CS1 assurance requirements

FC Reference	FC Assurance Element	CC Correspondence Notes
EPP-1.a	The developer shall provide documentation which describes the correspondence between the functional component requirements and the TCB elements and interfaces.	Covered in ASE class and ADV_RCR.1 and ADV_FSP
EPP-1.b	The TCB properties, which are defined by this correspondence, shall be explained in this documentation.	Covered in ASE class and ADV_RCR.1 and ADV_FSP
EPD-1.a	The developer shall provide an accurate description of the functions, effects, exceptions and error messages visible at the TCB interface.	Equivalent to requirement to provide 'an informal presentation of the syntax and semantics of all external /tsf interfaces.
EPD-1.b	The developer shall provide a list of the TCB elements (hardware, software, and firmware).	The CC CM requirements cover this issue but do not detail the contents of the configuration list, only that it describe the items that comprise the TSF.
EFT-1	The developer shall provide evidence of the functional testing that includes the test plan, the test procedures, and the results of the functional testing.	Covered under ATE_FUN.1
TA-1.a	The evaluator shall assess whether the producer has performed the activities defined in the development assurance requirements of the protection profile for functional testing and whether the producer has documented these activities as defined in the development evidence requirements of the protection profile.	Equivalent to ATE_FUN.1
TA-1.b	The evaluator shall analyze the results of the producer's testing activities for completeness of coverage and consistency of results.	Equivalent to ATE_FUN.1
TA-1.c	The evaluator shall determine whether the product's protection properties, as described in the product documentation have been tested.	Equivalent to ATE_FUN.1
TA-1.d	The evaluator shall assess testing results to determine whether the product's TCB works as claimed.	Equivalent to ATE_FUN.1
IT-1.a	A tester, independent of the producer or evaluator, shall perform functional and elementary penetration testing.	Not clear what 'independent of the producer or evaluator means'. ATE_IND.1 and AVA_VLA.1 deal with independent and penetration testing.

Table A.4 - Mapping to FC/CS1 assurance requirements

FC Reference	FC Assurance Element	CC Correspondence Notes
IT-1.b	This testing shall be based on the product's user and administrative documentation, and on relevant known penetration flaws.	This is partly addressed in AVA_MSU.1 for documentation vulnerabilities and partly in AVA_VLA.1 for penetration testing.
IT-1.c	Satisfactory completion consists of demonstrating that all user-visible security enforcing functions and security-relevant functions work as described in the product's user and administrative documentation and that no discrepancies exist between the documentation and the product.	Addressed as the outcome of ATE_FUN.1 for functional testing, and AVA_VLA.1 for vulnerability analysis. The documentation correctness is not specifically identified as a testing issue in the CC, this is covered under the general requirements for correctness of refinement.
IT-1.d	Test results of the producer shall be confirmed by the results of independent testing. The evaluator may selectively reconfirm any test result.	Equivalent to ATE_IND.1
IT-1.e	If the independent testing is performed at beta-test sites, the producer shall supply the beta-test plan and the test results.	Beta testing is not specifically mentioned as a separate topic, the independent test requirement remains. Beta testing can be regarded as one of the possible testing approaches which is compliant.
IT-1.f	The evaluator shall review the scope and depth of beta testing with respect to the required protection functionality, and shall verify independence of both the test sites and the producer's and beta-test user's test results.	Not specifically mentioned, the independent test requirement remains.
IT-1.g	The evaluator shall confirm that the test environment of the beta-test site(s) adequately represents the environment specified in the protection profile.	Not specifically mentioned, the independent test requirement remains.

Table A.4 - Mapping to FC/CS1 assurance requirements

588 The following discrepancies were noted between FC/CS1 and CC/CS1 assurance:

- a) FC/CS1 requires code and data structures to be defined whereas CC/CS1 does not require code and low level design to be evaluated.
- b) FC/CS1 is specific with respect to CM tracking, FC/CS1 does not specify the detail and leaves it to the developer to make representations about the CM capabilities.

- c) FC/CS1 lays greater stress on the lower level properties of the TCB interface (essentially the API), CC/CS1 does not call for the specific detail by name, only that the 'syntax and semantics' be defined.
- d) FC/CS1 does not require testing to the depth offered by CC/CS1. FC only tests the TSFI, CC tests at the high level design.
- e) FC/CS1 explicitly calls out a correction and re-test cycle as part of the testing, CC/CS1 has this implicitly in requiring that the testing should show a positive outcome.
- f) FC/CS1 requires user guidance to call out 'user responsibilities', this is not explicitly called out in the CC, the CC requirements can be viewed as equivalent.
- g) FC/CS1 requires the environmental issues to be discussed in the user guidance. CC/CS1 does not and leaves it to the environment to provide this.
- h) The FC/CS1 requirement on the trusted facility manual, and the CC/CS1 requirements on Administrator guidance are attempting to achieve the same result but the details of the required content differ. The end result is likely to be very similar though the criteria have significant differences of detail.
- i) The FC/CS1 has a number of specific requirements if beta testing is offered as the independent testing. This is not considered explicitly in the CC. Beta testing results can be used but the evaluator must make a judgement about adequacy and independence.

589 None of the above is of material significance, the effective assurance is at least equivalent though the FC has more prescriptive detail in some areas, and less in others.

590 The CC requires more design depth to be presented and may offer greater assurance at some greater cost but this may be offset by the FC requirement to reveal more of the code level implementation.

Annex B

Rationale for CS3 Protection Profile

B.1 Introduction

- 591 This rationale material is evaluation evidence and is included as an example of how
such rationale might be presented.
- 592 Rationale would not normally be included in the published PP but should be made
available to profile users by the registration authorities as required.
- 593 As an aid to evaluation, it is divided into sections which parallel the APE assurance
class. Readers and potential evaluators of this PP are invited to comment upon the
presentation, utility, and completeness of this material.

B.2 CS3 Security objectives

- 594 The CC requires that the PP security objectives are properly categorised as applied
to the TOE or its security environment, are useful and meaningful objectives, and
can be shown to cover all of the threats and organisational security policies
identified.
- 595 No specific evidence is offered in support of any claims of utility of the stated
security objectives. The rationale aims to demonstrate that the objectives identified
provide a complete coverage of the threats and policies.

B.2.1 Satisfaction of organisational security policies

- 596 This section demonstrates that a TOE (in its environment) which meets all of the
stated security objectives will effectively meet all of the identified organisational
security policies.

P.OWNER The organisation is the 'owner' of information and controls all access to it.

- 597 O.ROLE ensures that no user may perform any operation on an object without
being assigned to a role permitting that operation.

P.KNOWN Legitimate users of the system must be identified before rights of access can be
granted.

- 598 O.LOGICAL ensures that unknown persons can be denied the relevant access.

- 599 O.LOCATE ensures that users may be further identified and controlled by entry
device location.

600 O.OPERATE ensures the continuing correct operation of TOE security functions, including identification and authentication.

601 O.CREDEN (Environment) asserts that users do not have access to stolen, forged, or otherwise improperly obtained authentication tokens.

P.ROLE Rights for users to gain access to and perform operations on information must be based on identity-based 'need-to-know' and assigned role with respect to the information.

602 O.ROLE ensures that no user may perform any operation on an object without being assigned to a role permitting that operation.

603 O.ROLEDEV (Environment) directly asserts that the TOE management will develop and assign roles in a manner which maintains security.

P.DUTY Important information must be protected by 'separation of duties', such that no single user may be granted the right to perform all operations on it.

604 O.ROLEDEV (Environment) directly asserts that the TOE management will develop and assign roles in a manner which maintains security.

P.ACCOUNT Users must be held accountable for the security relevant actions they perform.

605 O.RECORD ensures that the TOE collects data necessary to identify security relevant actions by users.

606 O.ACCOUNT ensures that the TOE can enforce such a policy.

B.2.2 Threats to be addressed by the TOE

607 This section demonstrates that a TOE (in its environment) which meets all of the stated security objectives will effectively counter all of the identified threats.

T.ACCESS An unauthorised person may gain logical access to the TOE.

608 O.LOGICAL counters T.ACCESS explicitly.

609 O.RECORD leads to capture of a record of events which TOE management might consider suspicious and indicative of possible attempted intrusions.

610 O.FLAW controls flaws in the TOE which might permit intrusion.

611 O.CONTROL ensures that the management capabilities exist to permit observation and control of potential intrusion attempts.

612 O.OBSERVE ensures that the security administrator may readily observe and control the TOE security state, such as user/object policy attributes, system entry parameters necessary to provide effective access controls.

- 613 O.OPERATE ensures the continuing correct operation of TOE security functions, including identification and authentication.
- 614 O.MANAGE (Environment) asserts that the management support can and does control intrusion.
- 615 O.PHYSICAL (Environment) asserts that potential intruders cannot gain access through direct assault on the TOE.
- 616 O.CREDEN (Environment) asserts that intruders do not have access to stolen, forged, or otherwise improperly obtained authentication tokens.
- 617 O.CONNECT (Environment) asserts that intrusion emanating from uncontrolled network sources is controlled.
- T.AUTHOR** A user may gain access to resources or perform operations for which no access rights have been granted.
- 618 O.LOCATE permits users to be controlled by access time window and entry device location.
- 619 O.ROLE counters T.AUTHOR directly.
- 620 O.RECORD ensures that the TOE collects data necessary to detect apparent penetration attempts by legitimate users.
- 621 O.ACCOUNT ensures that any apparent penetration attempts can be traced to the offending user.
- 622 O.BYPASS ensures that the functions and facilities offered to legitimate users by the TOE cannot be misused contrary to the security policy.
- 623 O.FLAW ensures that the TOE contains no residual flaws which could be exploited by a user.
- 624 O.CONTROL asserts that the TOE management possesses the necessary management tools to ensure that the TOE enforces the security policy.
- 625 O.OPERATE ensures the continuing correct operation of TOE security functions, including access authorisation.
- 626 O.OBSERVE ensures that the security administrator may readily observe and control the TOE security state, such as user/object policy attributes, system entry parameters necessary to provide effective access controls.
- 627 O.MANAGE (Environment) asserts that the management support will control users adequately.

- 628 O.ROLEDEV (Environment) directly asserts that the TOE management will develop and assign roles in a manner which maintains security.
- 629 O.CREDEN (Environment) asserts that users do not have access to stolen, forged, or otherwise improperly obtained authentication tokens.
- T.TRACE** Security relevant events may not be recorded or may not be traceable to the user associated with the event.
- 630 O.ROLE ensures that a user may not gain access to any record of attempted intrusion to expunge it.
- 631 O.RECORD directly addresses this threat by ensuring that the TOE can collect information on security relevant events.
- 632 O.ACCOUNT ensures that, in the event of an attempted insider attack, the event is traceable to the correct miscreant.
- 633 O.BYPASS ensures that it is not possible to avoid creation of the evidence of intrusion.
- 634 O.FLAW ensures that undiscovered flaws cannot be exploited to cover an intruder's tracks.
- 635 O.CONTROL ensures that the TOE management possesses the necessary facilities to identify miscreants.
- 636 O.OPERATE ensures the continuing correct operation of TOE security functions, including auditability.
- 637 O.OBSERVE ensures that the security administrator may readily observe and control the TOE security state, such as selection of auditable events and management of audit data.
- 638 O.MANAGE (Environment) asserts that the management support is available to enforce proper record keeping.
- 639 O.CREDEN (Environment) asserts that users do not have access to stolen, forged, or otherwise improperly obtained authentication tokens.
- 640 O.CONNECT (Environment) asserts that intrusion emanating from uncontrolled network sources is controlled.
- T.FLAW** Security failures may occur because of flaws in the TOE.
- 641 O.FLAW ensures that no such flaws exist.
- T.DENY** Users may be denied accessibility to the resources of the TOE.

642 O.ACCESS ensures the continued accessibility of TOE resources by authorised users.

T.CRASH The secure state of the TOE could be compromised in the event of a system crash.

643 O.PRESERV ensures the preservation of the TOE in the event of a system failure or discontinuity of service.

T.TAMPER Protection relevant mechanisms of the TOE could be tampered with.

644 O.TAMPER counters this threat directly by preventing the tampering with protection relevant mechanisms.

T.OBSERVE Events may occur in TOE operation that compromise IT security but which may not be readily noticed.

645 O.OBSERVE directly counters this threat by ensuring that the security status of the TOE is readily observable and controllable by the system administrator.

B.2.3 Threats to be addressed by the operating environment

646 This section demonstrates that the threats to be countered by the security environment of the TOE map to the security objectives identified for the environment.

T.INSTALL The TOE may be delivered and installed in a manner which undermines security.

647 O.INSTALL (Environment) asserts that the TOE will be delivered and installed in a manner which maintains security.

T.PHYSICAL Security-critical parts of the TOE may be subjected to physical attack which may compromise security.

648 O.PHYSICAL (Environment) asserts that the TOE management will put the necessary physical controls in place.

649 O.MANAGE (Environment) asserts that the TOE management will continue to enforce the necessary physical controls.

T.OPERATE Security failures may occur because of improper administration and operation of the TOE.

650 O.MANAGE (Environment) directly asserts that TOE management accept the responsibility for countering this threat.

651 O.CREDEN (Environment) asserts that TOE users accept the responsibility for countering this threat by protection of access credentials.

652 O.CONNECT (Environment) asserts that the TOE management controls external connections which could impact upon the TOE security.

T.ROLEDEV The development and assignment of user roles may be done in a manner which undermines security.

653 O.ROLEDEV (Environment) directly asserts that the TOE management will develop and assign roles in a manner which maintains security.

B.2.4 Completeness of objectives

654 Table B.1 below shows the mapping of each objective to the threats and policies.

Security Objective	Threats	Organisational Security Policies
O.LOGICAL	T.ACCESS	P.KNOWN
O.LOCATE	T.AUTHOR	P.KNOWN
O.ROLE	T.AUTHOR T.TRACE	P.OWNER P.ROLE
O.RECORD	T.ACCESS T.AUTHOR T.TRACE	P.ACCOUNT
O.ACCOUNT	T.AUTHOR T.TRACE	P.ACCOUNT
O.TAMPER	T.TAMPER	
O.BYPASS	T.AUTHOR T.TRACE	
O.FLAW	T.ACCESS T.AUTHOR T.TRACE T.FLAW	
O.CONTROL	T.ACCESS T.AUTHOR	
O.OPERATE	T.ACCESS T.AUTHOR T.TRACE	P.KNOWN
O.ACCESS	T.DENY	
O.OBSERVE	T.ACCESS T.AUTHOR T.TRACE T.OBSERVE	

Table B.1 - Mapping objectives to threats and organisational security policies

Security Objective	Threats	Organisational Security Policies
O.PRESERV	T.TAMPER T.CRASH T.DENY T.FLAW T.OPERATE	
O.INSTALL (E)	T.INSTALL	
O.MANAGE (E)	T.AUTHOR T.TRACE	
O.PHYSICAL (E)	T.ACCESS T.PHYSICAL	
O.ROLEDEV (E)	T.AUTHOR T.ROLEDEV	P.ROLE P.DUTY
O.CREDEN (E)	T.ACCESS T.AUTHOR T.TRACE T.OPERATE	P.KNOWN
O.CONNECT	T.ACCESS T.TRACE T.OPERATE	

Table B.1 - Mapping objectives to threats and organisational security policies

655 Table B.1 indicates that all objectives contribute to the ability of the TOE to counter a threat and/or satisfy a policy and that all threats and policies have been addressed. Thus there are no unnecessary objectives.

656 No evaluation evidence is offered specifically in support of the claim that the objectives are sufficient to satisfy fully all threats and organisational security policies. Evaluators should consider the merits of the discussion of each threat and policy.

B.3 CS3 Functional requirements rationale

657 This section lists the individual components included in the profile and contains the full wording of the elements of those components.

658 Refinements of the element wording are indicated by italicising the refined text and, where necessary, explaining the refinement in following paragraphs.

659 Explanations of refinements and the justifications for the inclusion of the component are distinguished by the use of distinct fonts.

B.3.1 Identification and authentication requirements rationale**FIA_ADA.3 Expanded User Authentication Data Administration**

660 **FIA_ADA.3.1** The TSF shall provide functions for initialising and modifying user authentication data related to [assignment: *identified authentication mechanism*].

661 FIA_ADA.3.2 The TSF shall restrict use of these functions on the user authentication data for any user to the authorised administrator.

662 FIA_ADA.3.3 The TSF shall allow authorised users to use these functions to modify their own authentication data in accordance with the TSP.

663 Refinement:

- a) If passwords are used,
 - 1) The authorised user shall be allowed to modify his/her own authentication data within prescribed limits.
 - 2) The TSF shall provide a protected mechanism to allow a user to change his or her password. This mechanism shall require re-authentication of the user identity.

664 This component is a prerequisite to the entry objective O.LOGICAL, the access control objective O.ROLE, and the accountability objective O.ACCOUNT.

FIA_ADP.1 Basic User Authentication Data Protection

665 FIA_ADP.1.1 The TSF shall protect from unauthorised observation, modification and destruction authentication data that is stored in the TOE.

666 Refinement: The TSF shall store passwords in a one-way encrypted form.

667 Authentication depends upon the veracity, and possibly the secrecy, of authentication data. Thus unless adequate controls are imposed, the authentication requirements cannot be met.

668 This component is a prerequisite to the entry objective O.LOGICAL, the access control objective O.ROLE, and the accountability objective O.ACCOUNT.

FIA_ADP.2 Extended User Authentication Data Protection

669 FIA_ADP.2.1 The TSF shall protect from unauthorised observation, modification and destruction the raw form of authentication data at all times while it resides in the TOE.

670 Refinement:

- a) The TSF shall automatically suppress or fully blot out the clear-text representation of the password on the data entry/display device.

671 This component is a prerequisite to the entry objective O.LOGICAL, the access control objective O.ROLE, and the accountability objective O.ACCOUNT.

FIA_AFL.2 Administrator Controlled Authentication Failure Handling

672 FIA_AFL.2.1 The TSF shall be able to terminate the user session establishment process after [assignment: *number*] unsuccessful authentication attempts.

673 FIA_AFL.2.2 After the termination of a user session establishment process, the TSF shall provide the authorised administrator with the ability to specify whether the *user account* is to be disabled until [assignment: *conditions for re-enabling the user session establishment process*].

674 Refinement:

- a) The TSF shall appear to perform the entire user authentication procedure even if the user identification entered is invalid. Error feedback shall contain no information regarding which part of the authentication information is incorrect.
- b) The TSF shall end the attempted login session if the user performs the authentication procedure incorrectly for a number of successive times (i.e., a threshold) specified by an authorised system administrator. The default threshold shall be three times. When the threshold is exceeded, the TSF shall delay the next login by an interval of time specified by the authorised system administrator. The default time interval shall be 60 seconds.

675 This component is a prerequisite to the entry objective O.LOGICAL.

FIA_ATA1 Shared User Attribute Definitions

676 FIA_ATA.1.1 The TSF shall provide the ability to initialise user attributes with provided default values.

677 This will reduce the chance of selection of unsuitable user attributes by providing acceptable defaults.

678 This component is a prerequisite to the entry objective O.LOGICAL, the access control objective O.ROLE, and the accountability objective O.ACCOUNT.

FIA_ATA.2 Basic User Attribute Administration

679 FIA_ATA.2.1 The TSF shall provide the ability to display and modify user attributes.

680 FIA_ATA.2.2 The TSF shall limit the ability to modify user attributes to only the authorised administrator.

681 This component is a prerequisite to the entry objective O.LOGICAL, the access control objective O.ROLE, and the accountability objective O.ACCOUNT.

FIA_ATD.1 Shared User Attribute Definition

682 FIA_ATD.1.1 The TSF shall provide, for each user, a set of security attributes
necessary to enforce the TSP.

683 This component is a prerequisite to the entry objective O.LOGICAL, the access
control objective O.ROLE, and the accountability objective O.ACCOUNT.

FIA_ATD.2 Unique User Attribute Definition

684 FIA_ATD.2.1 The TSF shall provide, for each user, a unique set of security
attributes necessary to enforce the TSP.

685 This component is a prerequisite to the entry objective O.LOGICAL, the access
control objective O.ROLE, and the accountability objective O.ACCOUNT.

NOTE: If the TOE provides the capability for user-generated passwords, then the following
component FIA_SOS.1, Selection of Secrets, shall be selected. See section 3.7,
Application notes.

FIA_SOS.1 Selection of Secrets

686 FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet
[assignment: *a defined quality metric*].

687 Refinement:

- a) Passwords shall not be reusable by the same user identifier for a system-specifiable period of time. The default shall be six months.
- b) The TSF shall not indicate to the user if he/she has chosen a password already associated with another user.
- c) The TSF shall, by default, prohibit the use of null passwords during normal operation.
- d) The TSF shall provide an algorithm for ensuring the complexity of user-entered passwords that meets the following requirements:
 - 1) (1) Passwords shall meet a system-specifiable minimum length requirement. The default minimum length shall be eight characters.
 - 2) (2) The password complexity-checking algorithm shall be modifiable by the TSF. The default algorithm shall require passwords to include at least one alphabetic character, one numeric character, and one special character.
 - 3) (3) The TSF should provide a protected mechanism that allows systems to specify a list of excluded passwords (e.g., company acronyms, common surnames).

- 4) (a) The TSF should prevent users from selecting a password that matches any of those on the list of excluded passwords.
- e) The control of password complexity shall be limited to system administrators.

688 This component is a prerequisite to the entry objective O.LOGICAL, the access control objective O.ROLE, and the accountability objective O.ACCOUNT.

NOTE: If the TOE provides the capability for TSF-generated passwords, then the following component FIA_SOS.2, TSF Generation of Secrets, shall be selected. See section 3.7, Application notes.

FIA_SOS.2 TSF Generation of Secrets

689 FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet [assignment: *a defined quality metric*].

690 FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for [assignment: *list of TSF functions*].

691 Refinement:

- a) If password generation algorithms are present, they shall meet the following requirements:
 - 1) The password generation algorithm shall generate passwords that are easy to remember (i.e., pronounceable).
 - 2) The TSF should give the user a choice of alternative passwords from which to choose.
 - 3) Passwords shall be reasonably resistant to brute-force password guessing attacks.
 - 4) If the “alphabet” used by the password generation algorithm consists of syllables rather than characters, the security of the password shall not depend on the secrecy of the alphabet.
 - 5) The generated sequence of passwords shall have the property of randomness (i.e., consecutive instances shall be uncorrelated and the sequences shall not display periodicity).

692 This component is a prerequisite to the entry objective O.LOGICAL, the access control objective O.ROLE, and the accountability objective O.ACCOUNT.

FIA_UAU.1 Basic User Authentication

693 FIA_UAU.1.1 The TSF shall authenticate any user's claimed identity prior to performing any function for the user.

694 This component is a prerequisite to the entry objective O.LOGICAL, the access control objective O.ROLE, and the accountability objective O.ACCOUNT.

FIA_UAU.6 Configurable Authentication Mechanisms

695 FIA_UAU.6.1 The TSF shall provide [assignment: number] different mechanisms [assignment: list of different mechanisms] to authenticate any user's claimed identity.

696 FIA_UAU.6.2 The TSF shall enforce the use of [refinement: separate authentication mechanisms for specific authentication events], with authentication being successful if and only if all of the defined mechanisms individually indicate successful authentication.

697 FIA_UAU.6.2 The TSF shall allow the authorised administrator to associate [refinement: *separate authentication mechanisms with specific authentication events*].

698 This component is a prerequisite to the entry objective O.LOGICAL, the access control objective O.ROLE, and the accountability objective O.ACCOUNT.

FIA_UAU.9 Installable Authentication Mechanisms

699 FIA_UAU.9.1 The TSF shall provide the ability for the authorised administrator to incorporate installable authentication mechanisms into the TSF.

700 FIA_UAU.9.2 The TSF shall use the installed authentication mechanism in place of or in addition to any existing authentication mechanism.

701 This component is a prerequisite to the entry objective O.LOGICAL, the access control objective O.ROLE, and the accountability objective O.ACCOUNT.

FIA_UID.2 Unique Identification of Users

702 FIA_UID.2.1 The TSF shall uniquely identify each user before performing any actions requested by the user.

703 This component is a prerequisite to the entry objective O.LOGICAL, the access control objective O.ROLE, and the accountability objective O.ACCOUNT.

FIA_USB.1 User-Subject Binding

704 FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

705 This component is a prerequisite to the entry objective O.LOGICAL, the access control objective O.ROLE, and the accountability objective O.ACCOUNT.

B.3.2 TOE access requirements rationale**FTA_LSA.1 Limitation on Scope of Selectable Attributes**

706 FTA_LSA.1.1 The TSF shall restrict the scope of the session security attribute *role*, based on user identification.

707 FTA_LSA.1.2 Session establishment conditions shall be specifiable only by the authorised administrator.

708 This component is a prerequisite to the access control objective O.ROLE.

FTA_MCS.2 Per User Attribute Limitation on Multiple Concurrent Sessions

709 FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that can operate on behalf of a user based on the user's identity.

710 FTA_MCS.2.2 The TSF shall enforce, by default, a limit of a single session per user.

711 FTA_MCS.2.3 When more than one user session security attribute is applicable, the TSF shall use the minimum number of sessions.

712 FTA_MCS.2.4 Session establishment conditions shall be specifiable only by the authorised administrator.

713 This component is a prerequisite to the accessibility objective O.ACCESS.

NOTE: At least one of the following two components shall be selected: FTA_SSL.1 (TSF-initiated Session Locking) or FTA_SSL.3 (TSF-initiated Termination). See note on these two components in section 3.7, Application notes.

FTA_SSL.1 TSF-initiated Session Locking

714 FTA_SSL.1.1 The TSF shall lock an interactive session after a specified interval of user inactivity by:

- a) clearing or overwriting display devices, making the current contents unreadable;
- b) disabling any activity of the user's data access/display devices other than unlocking the session.

715 FTA_SSL.1.2 The default value for the user inactivity interval shall be specifiable only by the authorised administrator.

716 FTA_SSL.1.3 The TSF shall require user authentication prior to unlocking the session.

717 This component is a prerequisite to the entry objective O.LOGICAL and the access control objective O.ROLE.

FTA_SSL.3 TSF-initiated Termination

- 718 FTA_SSL.3.1 The TSF shall terminate an interactive session after a specified interval of user inactivity.
- 719 FTA_SSL.3.2 The default value for the user inactivity interval shall be specifiable only by the authorised administrator.
- 720 This component is a prerequisite to the entry objective O.LOGICAL and the access control objective O.ROLE.

FTA_SSL.2 User-initiated Locking

- 721 FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive sessions by:
- a) clearing or over-writing display devices, making the current contents unreadable;
 - b) disabling any activity of the user's data access/display devices other than unlocking the session.
- 722 FTA_SSL.2.2 The TSF shall require user authentication prior to unlocking the session.
- 723 This component is a prerequisite to the entry objective O.LOGICAL and the access control objective O.ROLE.

FTA_TAB.2 Configurable TOE Access Banners

- 724 FTA_TAB.2.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.
- 725 FTA_TAB.2.2 The default advisory warning message displayed by the TSF shall be as follows:
- a) NOTICE: This is a private computer system. All users of this system are subject to having their activities audited. Anyone using this system consents to such auditing. All unauthorised entries or activities revealed by this auditing can be used as evidence and may lead to criminal prosecution
- 726 FTA_TAB.2.3 The TSF shall restrict the capability to modify the warning message to the authorised administrator.
- 727 This component is a prerequisite to the entry objective O.LOGICAL.

FTA_TAH.1 TOE Access History

- 728 FTA_TAH.1.1 Upon successful session establishment, the TSF shall display the date, time, method, and location of the last successful session establishment to the user.

729 FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the date, time, method, location of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

730 FTA_TAH.1.3 The data specified above shall not be removed without user intervention.

731 This component is a prerequisite to the entry objective O.LOGICAL.

FTA_TAM.1 Basic TOE Access Management

732 FTA_TAM.1.1 The TSF shall restrict the capability to display and modify TOE access parameters to the authorised administrator.

733 FTA_TAM.1.2 The TSF shall allow the authorised administrators to display all TOE access parameters for a user, and users associated with a TOE access parameter.

734 This component is a prerequisite to the entry objective O.LOGICAL.

FTA_TSE.1 TOE session establishment

735 FTA_TSE.1.1 The TSF shall be able to deny session establishment based on time of access.

736 Refinement:

- a) Entry conditions using these ranges shall be specified using time-of-day, day-of-week, and calendar dates.

737 FTA_TSE.1.1 The TSF shall be able to deny session establishment based on originating location.

738 FTA_TSE.1.1 The TSF shall be able to deny session establishment based on method of access.

739 FTA_TSE.1.2 Session establishment conditions shall be specifiable only by the authorised administrator.

740 This component is a prerequisite to the time and entry device location objective O.LOCATE.

B.3.3 Trusted path requirements rationale

FTP_TRP.1 Trusted Path

741 FTP_TRP.1.1 The TSF shall provide a communication path between itself and local human users that is logically distinct from other communication paths and provides assured identification of its endpoints.

742 FTP_TRP.1.2 The TSF, and local users shall have the ability to initiate communication via the trusted path.

743 FTP_TRP.1.3 The TSF shall require initiation of the trusted path for initial user authentication, [assignment: *other services for which trusted path is required*].

744 This component is a prerequisite to the security policy enforcement objective O.BYPASS.

B.3.4 User data protection requirements rationale

FDP_ACC.1 Subset Object Access Control - RBAC

745 FDP_ACC.1.1 The TSF shall enforce the Role-Based Access Control (RBAC) SFP on:

- a) subjects acting on behalf of users
- b) [assignment: objects acted upon by RBAC operations]
- c) [assignment: *RBAC operations performed on objects covered by the RBAC FSP*].
- d) roles

746 This component is primarily directed against the access control objective O.ROLE.

FDP_ACF.1 Single Security Attribute Access Control - RBAC

747 FDP_ACF.1.1 The TSF shall enforce the RBAC SFP to objects based on the following subject attributes:

- a) user identity
- b) role(s)

748 FDP_ACF.1.1 The TSF shall enforce the RBAC SFP to objects based on the following object attributes:

- a) Object identifier.

749 FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

750 A subject operating in a role on behalf of a user can perform an operation on an object if:

- a) The user is an authorised member of the role, and
- b) The operation is an authorised operation for the role, and
- c) The object is authorised for the operation.

751 This component is primarily directed against the access control objective O.ROLE.

FDP_ACF.3 Access Authorization - RBAC

752 FDP_ACF.3.1 The TSF shall enforce the RBAC SFP to provide the ability to explicitly grant access based on the value of security attributes of subjects and objects.

753 This component is primarily directed against the access control objective O.ROLE.

FDP_ACC.1 Subset Object Access Control -- DAC

754 FDP_ACC.1.1 The TSF shall enforce the Discretionary Access Control (DAC) SFP on:

- a) subjects acting on behalf of users
- b) [assignment: list of other subjects]
- c) [assignment: list of objects]
- d) [assignment: operations among subjects and objects covered by the DAC SFP, e.g., read, write, execute].

755 This component is primarily directed against the access control objective O.ROLE.

FDP_ACF.1 Single Security Attribute Access Control - DAC

756 FDP_ACF.1.1 The TSF shall enforce the DAC SFP to objects based on the following subject attributes:

- a) user identity
- b) groups of which the user is a member

757 FDP_ACF.1.1 The TSF shall enforce the DAC SFP to objects based on the following object attributes:

- a) Access Control List: A list of user identities and/or a list of groups, and for each user identity and group entry, a list of permitted operations.
- b) A list of users and/or a list of groups that are explicitly denied access

758 FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

759 A subject is allowed to perform an operation on an object if:

- a) The subject's user identity is not on the list of users that are denied access to the object, and
- b) The subject's user identity is contained in the list of user identities of the object's ACL, or the user identity is a member of a group of the object's

ACL, and the operation is contained in the list of operations for the user's identity.

- c) Denial of access takes precedence over granting of access.

760 This component is primarily directed against the access control objective O.ROLE.

FDP_ACF.4 Access Authorization and Denial

761 FDP_ACF.4.1 The TSF shall enforce the DAC SFP to provide the ability to explicitly grant access based on the value of security attributes of subjects and objects.

762 FDP_ACF.4.2 The TSF shall provide the ability to explicitly deny access based on the value of security attributes of subjects and objects covered.

763 This component is primarily directed against the access control objective O.ROLE.

FDP_ACI.3 Basic Attribute Initialisation

764 FDP_ACI.3.1 The TSF shall enforce the Discretionary Access Control SFP to provide restrictive default values for security attributes that are used to enforce the SFP.

765 FDP_ACI.3.2 The TSF shall allow the specification of alternate initial values to override the default values when an object is created.

766 FDP_ACI.3.3 The TSF shall provide authorised users the capability to modify the default values of their related attributes.

767 This component is primarily directed against the access control objective O.ROLE.

FDP_RIP.2 Full Residual Information Protection

768 FDP_RIP.2.1 The TSF shall ensure that upon the [selection: *allocation, deallocation, allocation or deallocation*] of a resource to/from all objects any previous information content is unavailable.

769 This component has been included in answer to objective O.ROLE. It ensures that a particular class of implementation shortcoming does not undermine the access control policy and should also be traced to O.FLAW.

FDP_SAM.2 Basic Attribute Modification

770 FDP_SAM.2.1 The TSF shall enforce the Discretionary Access Control SFP to provide authorised users with the ability to modify access control lists created by the users.

771 This component is primarily directed against the access control objective O.ROLE.

FDP.SAM.3 Safe Attribute Modification

772 FDP.SAM.3.1 The TSF shall enforce the Role-Based Access Control SFP to verify that the modified values are valid when changes are made to the following:

- a) membership in roles,
- b) operations associated with roles,
- c) operations permitted for an object.

773 This component is primarily directed against the access control objective O.ROLE.

FDP_SAQ.1 Administrator Attribute Query

774 FDP_SAQ.1.1 The TSF shall enforce the Role-Based Access Control SFP to provide the authorised administrator with the ability to query the following attribute values:

- a) names of all roles,
- b) user members of a role,
- c) operations associated with a role,
- d) operations permitted on an object,
- e) objects accessible by a role.

775 This component is primarily directed against the access control objective O.ROLE.

FDP_SAQ.2 User Attribute Query

776 FDP_SAQ.2.1 The TSF shall enforce the Discretionary Access Control SFP to provide the authorised users with the ability to query the following attribute values:

- a) name of all groups,
- b) access control lists for objects that the user owns.

777 This component is primarily directed against the access control objective O.ROLE.

B.3.5 Audit requirements rationale

FAU_ARP.1 Security Alarms

778 FAU_ARP.1.1 The TSF shall immediately generate an alarm to the authorised administrator upon detection of events deemed to indicate a possible security violation.

779 Refinement:

- a) When the threshold for incorrect attempted login sessions is exceeded, the TSF shall send an alarm message to the system console and/or to the administrator's terminal

780 This component is primarily directed against the accountability objective O.ACCOUNT.

FAU_ARP.2 Automatic Response

781 FAU_ARP.2.1 The TSF shall take [assignment: *the least disruptive actions*] to terminate the occurrence of a relevant security event upon detection of a possible security violation.

782 Refinement:

- a) The TSF shall end an attempted login session if the user performs the authentication procedure incorrectly for a number of successive times (i.e., a threshold) specified by the authorised administrator. The default threshold shall be three times.
- b) When the threshold is exceeded, the TSF shall delay the next login by an interval of time specified by the authorized system administrator. The default time interval shall be 60 seconds.
- c) The TSF shall provide a protected mechanism to disable the user identity or account when the threshold of successive, unsuccessful login attempts is violated more than a number of times specified by the administrator. By default, this mechanism shall be disabled (as it may cause unauthorized denial of service)

783 This component is primarily directed against the accountability objective O.ACCOUNT.

FAU_GEN.1 Audit Data Generation

784 FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions.
- b) All auditable events relevant for the basic level of audit as defined in all functional components included in the PP/ST.
 - 1) [FIA_ADA] Any attempts to use TSF authentication data management mechanisms.
 - 2) [FIA_ADP] Successful attempts to access user authentication data.
 - 3) [FIA_ADP] All attempts by an unauthorised user to access user authentication data.

- 4) [FIA_ATA] All attempted uses of the user attribute administration function.
- 5) [FIA_ATA] Identification of the user attributes that have been modified.
- 6) [FIA_SOS] Rejection or acceptance by the TSF of any tested secret.
- 7) [FIA_UAU] Any use of the authentication mechanism.
- 8) [FIA_UAU] Audit the action of configuring the mapping of authentication mechanisms to specific authentication events.
- 9) [FIA_UAU] Installation of an authentication mechanism.
- 10) [FIA_UID] All attempts to use the user identification mechanism, including the user identity provided.
- 11) [FIA_USB] Success and failure of binding of user security attributes to a subject (e.g., creation of a subject).
- 12) [FTA_LSA] All attempts at selecting a user attribute based on the domain of selectable attributes.
- 13) [FTA_MCS] Rejection of a new session based on the limitation of multiple concurrent sessions.
- 14) [FTA_MCS] All attempts at establishment of a user session.
- 15) [FTA_SSL] Locking of an interactive session by the session locking mechanism.
- 16) [FTA_SSL] Successful unlocking of an interactive session.
- 17) [FTA_SSL] Termination of an interactive session by the session termination mechanism.
- 18) [FTA_TSE] All attempts at establishment of a user session.
- 19) [FTP_TRP] Identification of the initiator and target of the trusted channel.
- 20) [FTP_TRP] All attempted uses of the trusted channel functions.
- 21) [FDP_ACF] The security attributes used and the identity of any users, subjects, and/or objects involved in a successful mediation.
- 22) [FDP_ACF] Decisions to permit a requested operation.
- 23) [FDP_ACF] The security attributes used and the identity of any users, subjects, and/or objects involved in an unsuccessful mediation.

- 24) [FDP_ACF] Decisions to deny a requested operation.
- 25) [FDP_ACF] The identity of a user or subject unsuccessfully attempting to export an object.
- 26) [FDP_SAM] The identity of a user and/or subject successfully modifying security attributes and the target of the modification.
- 27) [FDP_SAM] Unsuccessful attempts to change security attributes.
- 28) [FDP_SAM] The new values of modified security attributes.
- 29) [FDP_SAM] The identity of a user and/or subject unsuccessfully attempting to modify security attributes, the target of the attempted modification, and the old and requested new value of the attribute.
- 30) [FDP_SAQ] The identity of a user successfully querying security attributes and the target of the query.
- 31) [FDP_SAQ] The identity of a user unsuccessfully querying security attributes and the target of the query.
- 32) [FAU_ARP] Generation of an alarm to the administrator when a security violation appears imminent.
- 33) [FAU_ARP] Successful application of the least disruptive action that should be taken when a security violation appears imminent.
- 34) [FAU_MGT] Any attempt to perform an operation on the audit trail.
- 35) [FAU_MGT] Notification of the authorised administrator in case of audit trail saturation.
- 36) [FAU_PAD] Enabling and disabling of any of the anomaly detection analysis mechanisms.
- 37) [FAU_PAD] Notifications made to the authorised administrator by the anomaly detection mechanisms.
- 38) [FAU_PAD] Automated responses made by the anomaly detection mechanisms.
- 39) [FAU_PAD] Any changes made to the configuration of the anomaly detection mechanisms.
- 40) [FAU_PIT] Enabling and disabling of any of the penetration identification analysis mechanisms.
- 41) [FAU_PIT] Notifications made to the authorised administrator by the penetration identification analysis mechanisms.
- 42) [FAU_PRO] Any attempt to read, modify, or destroy the audit trail.

- 43) [FAU_SAA] Detection of imminent violation by the security audit analysis mechanisms.
 - 44) [FAU_SEL] All modifications to the audit configuration that occur while the audit collection functions are operating.
 - 45) [FPT_SAE] Specification of the expiration time for a security attribute.
 - 46) [FPT_TDC] Any use of the TSF data consistency mechanisms.
 - 47) [FPT_TDC] Identification of which TSF data have been interpreted.
 - 48) [FPT_TDC] Detection of modified TSF data.
 - 49) [FPT_TSA] Use of a security-relevant administrative function.
 - 50) [FPT_TSA] The designation of a function as a security-relevant administrative function.
 - 51) [FPT_TSA] Explicit requests to assume the security administrative role.
 - 52) [FRU_RSA] All attempted uses of the resource allocation functions for resources that are under the control of the TSF.
- c) Other auditable events defined below:
- 1) [FPT_AMT] Use and result of the self test functions
 - 2) [FPT_TSA] [assignment: *actions taken by computer operators and system administrators and/or system security officers*]
 - 3) [assignment: *other auditable events*]

785

Refinement:

- a) The TSF shall support an application program interface that allows a privileged application to append data to the security audit trail or to an applications-specified alternative security audit trail.

786

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity, and [selection: *success, failure*] of the event.
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

787

This component is primarily directed against the security event recording objective O.RECORD and the accountability objective O.ACCOUNT.

FAU_GEN.2 Individual Identity Generation

788 FAU_GEN.2.1 The TSF shall be able to associate any auditable events with the individual identity of the user that caused the events.

789 This component is primarily directed against the security event recording objective O.RECORD and the accountability objective O.ACCOUNT.

FAU_MGT.1 Audit Trail Management

790 FAU_MGT.1.1 The TSF shall provide the authorised administrator with the ability to [selection: *create, delete, empty*] the audit trail.

791 Refinement:

a) The audit trail management tools shall enable:

- 1) Creation, destruction, and emptying of audit trails.
- 2) Modification of the audit trail size.
- 3) Formatting and compressing of event records.
- 4) Displaying of formatted audit trail data.
- 5) Automatic copying of security audit trail files to an alternative storage area after a system-specifiable period of time.
- 6) Automatic deletion of security audit trail files after a system-specifiable period of time. The default shall be thirty days.
- 7) It shall not be possible to delete the security audit trail before it gets copied to an alternate storage area. It shall be possible to disable this mechanism.
- 8) Maintaining the consistency of the audit trail data after system failures and discontinuity of operation.

792 This component is primarily directed against the security event recording objective O.RECORD. It should also be applied to the security management objective O.CONTROL.

FAU_MGT.3 Audit Trail Saturation Management

793 FAU_MGT.3.1 The TSF shall generate an alarm to the authorised administrator if the size of the audit data in the audit trail exceeds a pre-defined limit.

794 FAU_MGT.3.2 The TSF shall provide the authorised administrator with the ability to specify the pre-defined limit of the audit data in the audit trail at which point an alarm will be generated.

795 This component is primarily directed against the security event recording objective O.RECORD. It should also be applied to the security management objective O.CONTROL.

FAU_PAD.1 Profile Based Anomaly Detection

796 FAU_PAD.1.1 The TSF shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [assignment: *specify the profile target group*].

797 FAU_PAD.1.2 The TSF shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.

798 FAU_PAD.1.3 The TSF shall be able to indicate an imminent violation of the TSP when a user's suspicion rating exceeds the following threshold conditions [assignment: *conditions under which anomalous activity is reported by the TSF*].

799 Refinement:

- a) The TSF shall identify the number of successive incorrect attempted login sessions by a single user identity and compare that number against a threshold specified by an authorised administrator. The default threshold shall be three times.

800 This component is primarily directed against the entry objective O.LOGICAL.

FAU_PIT.1 Simple Attack Heuristics

801 FAU_PIT.1.1 The TSF shall be able to maintain an internal representation of the following signature events [assignment: *a subset of system events*] that may indicate a violation of the TSP.

802 Refinement:

- a) Successive incorrect login attempts by a single user identity.

803 FAU_PIT.1.2 The TSF shall be able to compare the signature events against the record of system activity discernable from an examination of [assignment: *specify the information to be used to determine system activity*].

804 Refinement:

- a) Audit records of failed login attempts.

805 FAU_PIT.1.3 The TSF shall be able indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.

806 This component is primarily directed against the entry objective O.LOGICAL.

FAU_PRO.2 Extended Audit Trail Access

- 807 FAU_PRO.2.1 The TSF shall restrict full access to the audit trail to the authorised administrator.
- 808 FAU_PRO.2.2 The TSF shall provide only authorised users with the capability to read [assignment: *list of audit information*] from the audit trail.
- 809 This component is primarily directed against the accountability objective O.ACCOUNT.

FAU_SAA.1 Imminent Violation Analysis

- 810 FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.
- 811 FAU_SAA.1.2 The set of rules shall be:
- a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a possible or imminent security violation;
 - b) Refinement:
Successive incorrect login attempts by a single user identity.
 - c) [Assignment: *any other rules*].
- 812 This component is primarily directed against the entry objective O.LOGICAL.

FAU_SAR.2 Extended Audit Review

- 813 FAU_SAR.2.1 The TSF shall provide audit review tools, with the ability to view the audit data.
- 814 FAU_SAR.2.2 The TSF shall restrict full use of the audit review tools to the authorised administrator.
- 815 FAU_SAR.2.3 The TSF shall provide only authorised users with limited use of the audit review tools.
- 816 This component is primarily directed against the accountability objective O.ACCOUNT and the status observability objective O.OBSERVE.

FAU_SEL.1 Selective Audit

- 817 FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
- a) [selection: *object identity, user identity, subject identity, host identity, event type*];

b) [assignment: *list of additional attributes*] that audit selectivity is based upon.

818 This component is primarily directed against the security event recording objective O.RECORD.

FAU_SEL.2 Runtime Selection Mode

819 FAU_SEL.2.1 The TSF shall provide the authorised administrator with the capability to select, at any time during the operation of the TOE, which events are to be audited.

820 This component is primarily directed against the security event recording objective O.RECORD.

FAU_SEL.3 Restricted Runtime Display Mode

821 FAU_SEL.3.1 The TSF shall restrict to the authorised administrator the capability to display, at any time during the operation of the TOE, which events are being audited.

822 This component is primarily directed against the accountability objective O.ACCOUNT and the status observability objective O.OBSERVE.

FAU_STG.1 Permanent Audit Trail Storage

823 FAU_STG.1.1 The TSF shall store generated audit records in a permanent audit trail.

824 This component is primarily directed against the security event recording objective O.RECORD.

FAU_STG.3 Prevention of Audit Data Loss

825 FAU_STG.3.1 The TSF shall limit the number of audit records lost due to system [selection: *audit storage exhaustion, failure, attack*].

826 FAU_STG.3.2 In the event of audit storage exhaustion, the TSF shall be capable of [selection: *ignoring, preventing*] the occurrence of auditable actions, except those taken by the authorised administrator.

827 This component is primarily directed against the security event recording objective O.RECORD.

B.3.6 Protection of TSF requirements rationale

FPT_AMT.3 Abstract Machine Testing During Normal Operation

828 FPT_AMT.3.1 The TSF shall provide the authorised administrator with the capability to demonstrate the correct operation of the security-relevant functions provided by the TSF's underlying abstract machine.

829 FPT_AMT.3.2 The TSF shall run a suite of self tests during initial start-up and periodically during normal operation in order to demonstrate the correct operation of the functions provided by the TSF's underlying abstract machine.

830 This component has been included primarily in answer to the correct operation objective O.OPERATE, although it is also responsive to O.FLAW, as hardware failure is an (albeit temporary) implementation flaw.

FPT_FLS.1 Failure with Preservation of Secure State

831 FPT_FLS.1.1 The TSF shall preserve secure state when [assignment: *list of types of TSF failures.*] failures occur.

832 This component has been included in answer to the correct operation objective O.OPERATE.

FPT_PHP.1 Passive Detection of Physical Attack

833 FPT_PHP.1.1 The TOE shall include features that provide unambiguous detection of physical tampering with the TSFs physical devices and elements.

834 FPT_PHP.1.2 The TSF shall provide the authorised administrator with the capability to determine whether physical tampering to the TSF's devices and elements has been detected.

835 This component is directed against the physical tampering objective O.TAMPER.

FPT_RCV.2 Automated Recovery

836 FPT_RCV.2.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

837 FPT_RCV.2.2 The TSF shall provide the authorised administrator with the capability to restore the TSF data to a consistent and secure state.

838 FPT_RCV.2.3 For [assignment: *list of failures/service discontinuities*], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

839 This component is directed against the secure state objective O.PRESERV.

FPT_RVM.1 Non-Bypassability of the TSP

840 FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before any security-related action is allowed to proceed.

841 This component is necessary in order to be able to reason about the access control policy enforcement objective O.ROLE. The corresponding control objective is O.BYPASS.

FPT_SAE.1 Time-Limited Authorisation

842 FPT_SAE.1.1 The TSF shall provide a capability for the authorised administrator to specify an expiration time for [assignment: *list of security attributes for which expiration is to be supported*].

843 FPT_SAE.1.2 For each of these security attributes, the TSF shall be able to [assignment: *list of actions to be taken for each security attribute*] after the expiration time for the indicated security attribute has passed.

844 Refinements:

- a) The TSF shall enforce password aging on a per- user identifier, per-group, or per-role basis (i.e., a user shall be required to change his or her password after a system-specifiable minimum time). The default for all non-system administrators shall be sixty days.
 - 1) The default for system administrator identifiers shall be thirty days.
 - 2) After the password aging threshold has been reached, the password shall no longer be valid, except as provided in 5 g below.
- b) The TSF shall provide a protected mechanism to notify users in advance of requiring them to change their passwords. This can be done by either:
 - 1) Notifying users a system-specifiable period of time prior to their password expiring. The default shall be seven days.
 - or -
 - 2) Upon password expiration, notifying the user but allowing a system-specifiable subsequent number of additional logons prior to requiring a new password. The default shall be two additional logons.
- c) The control of user password expiration defaults shall be limited to system administrators.

845 This objective is directed against the access objective O.LOGICAL.

FPT_SEP.1 TSF Domain Separation

846 FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

847 FPT_SEP.1.2 The TSF shall enforce separation between the address spaces of subjects in the TSC.

848 This component is necessary in order to be able to reason about the access control policy enforcement objective O.ROLE. The corresponding control objective is O.BYPASS.

FPT_SWM.1 Protection of Executables

849 FPT_SWM.1.1 The TSF shall provide the authorised administrator with the capability to verify the integrity of stored TSF executable code.

850 This component has been included in answer to the correct operation objective O.OPERATE.

FPT_TDC.1 Inter-TSF Basic TSF Consistency

851 FPT_TDC.1.1 The TSF shall enforce the consistent interpretation of [assignment: *list of TSF data types*] during inter-TSF transfers.

852 FPT_TDC.1.2 The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data during inter-TSF transfers.

853 This component has been included in answer to the entry objective O.LOGICAL and the access control objective O.ROLE.

FPT_TSA.2 Separate Security Administrative Roles

854 FPT_TSA.2.1 The TSF shall distinguish security-relevant administrative functions from other functions.

855 FPT_TSA.2.2 The TSF's set of security-relevant administrative functions shall include all functions necessary to install, configure, and manage the TSF; minimally, this set shall include [assignment: *list of services to be minimally supplied*].

856 FPT_TSA.2.3 The TSF shall restrict the ability to use security-relevant administrative functions to a security administrative role that has a specific set of authorised functions and responsibilities.

857 FPT_TSA.2.4 The TSF shall be capable of distinguishing the set of users authorised for administrative functions from the set of all users of the TOE.

858 FPT_TSA.2.5 The TSF shall allow only specifically authorised users to assume the security administrative role.

859 FPT_TSA.2.6 The TSF shall require an explicit request to be made in order for an authorised user to assume the security administrative role.

860 This component is directed against the security management objective O.CONTROL, although adequate administration capability is a general requirement which contributes to the meeting of all security objectives.

FPT_TSM.1 Management Functions

861 FPT_TSM.1.1 The TSF shall provide the authorised administrator with the ability to set and update the following TSF configuration parameters:

- a) The authentication method on a per policy-attribute basis whenever multiple authentication methods are used for FIA_UAU

- b) Session establishment conditions to limit the scope of selectable attributes for FTA_LSA.1..
- c) Per user attribute limitations on multiple concurrent sessions for FTA_MCS.2
- d) The default value for the user activity interval for FTA_SSL.1 or FTA_SSL.3
- e) The warning message for FTA_TAB.2
- f) The time of access, originating of access, and method of access conditions for FTA_TSE.1
- g) The audit trail parameter for FAU_MGT.1
- h) The pre-defined limit of the audit data in the audit trail for FAU_MGT.3.
- i) assigning: [*other TSF configuration parameters*].

862 FPT_TSM.1.2 The TSF shall provide the authorised administrator with the ability to perform the following administrative functions:

- a) Create named groups.
- b) Delete named groups
- c) Authorise users into one or more named groups.
- d) Create named roles.
- e) Delete named roles.
- f) Authorise users into one or more named roles.
- g) Authorise one or more role operations for a role.
- h) Authorise one or more operations that can be performed on a role.
- i) [assignment: *other administrative functions*].

863 This component is directed against the security management objective O.CONTROL and the related status observability objective O.OBSERVE.

FPT_TST.3 TSF Testing During Normal Operation

864 FPT_TST.3.1 The TSF shall provide authorised administrators with the capability to demonstrate the correct operation of the TSF.

865 FPT_TST.3.2 The TSF shall provide authorised administrators with the capability to verify the integrity of TSF data.

866 FPT_TST.3.3 The TSF shall exercise a suite of self tests during initial start-up and periodically during normal operation in order to demonstrate the correct operation of the TSF.

867 Refinements:

- a) Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TSF. These features shall include: power-on tests, loadable tests, and operator-controlled tests.
- b) The power-on tests shall test all basic components of the TSF hardware and firmware elements including memory boards and memory interconnections; data paths; busses; control logic and processor registers; disk adapters; communication ports; system consoles, and the keyboard speaker. These tests shall cover all components that are necessary to run the loadable tests and the operator-controlled tests.
- c) The loadable tests shall cover: processor components (e.g., arithmetic and logic unit, floating point unit, instruction decode buffers, interrupt controllers, register transfer bus, address translation buffer, cache, and processor-to-memory bus controller); backplane busses; memory controllers; writable control memory for operator-controlled and remote system-integrity testing.
- d) Operator-controlled tests shall be able to initiate a series of one-time or repeated tests, to log the results of these tests and, if any fault is detected, to direct the integrity-test programs to identify and isolate the failure. The execution of operator-controlled tests shall be limited to system operators.

868 This component is directed against the secure operation objective O.OPERATE, although it is also potentially supportive of the anti-tampering objective O.TAMPER.

FPT_TSU.1 Enforcement of Administrative Guidance

869 FPT_TSU.1.1 The TSF shall enforce checks for valid input values for security-relevant administrative functions as described in the Administrative Guidance.

870 This component is directed against the security management objective O.CONTROL. The general administration requirements contribute to all objectives by reducing the probability of operator errors leading to insecure configuration.

B.3.7 Resource utilisation requirements rationale

FRU_RSA.1 Maximum Quotas

871 FRU_RSA.1.1 The TSF shall enforce quotas limiting the maximum quantity of [assignment: *controlled resources*] that [selection: *individual user, defined group of users*] can use [selection: *simultaneously, over a specified period of time*].

872 This component is directed against the resource accessibility objective O.ACCESS.

873 B.4 Satisfaction of IT security objectives

873 The following table B.1 portrays the relationship of the functional requirements components to the CS3 IT security objectives they are intended to satisfy.

874 Every IT security objective is shown to be met by at least one functional requirement component. The analysis previously given in section B.3 demonstrated the reverse argument, that every functional requirement is supportive of at least one IT security objective.

Security Objective	Functional Requirement Components
O.LOGICAL The TOE must strongly prevent logical entry to it by persons or processes with no rights to access it.	FIA_ADA.3, FIA_ADP.1&2 FIA_AFL.2, FIA_ATA.1&2 FIA_ATD.1&2, FIA_SOS.1&2 FIA_UAU.1-6-9, FIA_UID.2 FIA_USB.1, FTA_SSL.1-2-3 FTA_TAB.2, FTA_TAH.1 FTA_TAM.1, FAU_PAD.1 FAU_SAA.1, FPT_SAE.1 FPT_TDC.1
O.LOCATE The TOE must be able to restrict user entry to it based on time and entry device location.	FTA_TSE.1
O.ROLE The TOE must prevent users from gaining access to and performing operations on its resources for which their role does not have explicit permission.	FIA_ADA.3, FIA_ADP.1&2 FIA_AFL.2, FIA_ATA.1&2 FIA_ATD.1&2, FIA_SOS.1&2 FIA_UAU.1-6-9, FIA_UID.2 FIA_USB.1, FTA_LSA.1 FTA_SSL.1-2-3, FDP_ACC.1 FDP_ACF.1-2-3, FDP_SAM.1-2-3 FDP_SAQ.1-2, FPT_SEP.1 FPT_TDC.1
O.RECORD The TOE must record necessary events to ensure that the information exists to support effective security management.	FAU_GEN.1-2 FAU_MGT.1-3 FAU_SEL.1-2 FAU_STG.1-3

Table B.2 - Mapping objectives to functional requirements

Security Objective	Functional Requirement Components
O.ACCOUNT The TOE must ensure that all users can be held accountable for their security relevant actions.	FIA_ADA.3, FIA_ADP.1&2 FIA_AFL.2, FIA_ATA.1&2 FIA_ATD.1&2, FIA_SOS.1&2 FIA_UAU.1-6-9, FIA_UID.2 FIA_USB.1, FAU_ARP.1-2 FAU_GEN.1-2, FAU_PRO.2 FAU_SAR.2, FAU_SEL.3
O.TAMPER The TOE must prevent physical tampering with its security-critical parts.	FPT_PHP.1 FPT_TST.3
O.BYPASS The TOE must prevent illicit or errant software or users from bypassing TOE security policy enforcement.	FPT_RVM.1 FPT_SEP.1 FPT_TRP.1
O.FLAW The TOE must not contain flaws in design, implementation, or operation.	[Assurance Level EAL4] FDP_RIP.2 FPT_AMT.3
O.CONTROL The TOE must provide all the functions and facilities necessary to support those responsible for the management of TOE security.	FAU_MGT.1-3 FPT_TSA.2 FPT_TSM.1 FPT_TSU.1
O.OPERATE The TOE must ensure the continued correct operation of its security functions	FPT_AMT.3 FPT_FLS.1 FPT_SWM.1 FPT_TST.3
O.ACCESS The TOE must ensure the continued accessibility of TOE resources by authorised users.	FTA_MCS.2 FRU_RSA.1
O.OBSERVE The TOE must ensure that its security status is readily observable and controllable by the system administrator at all times.	FAU_SAR.2 FAU_SEL.3 FPT_TSM
O.PRESERV The TOE must ensure that its secure state is preserved in the event of a system failure or discontinuity of service.	FPT_RCV.2

Table B.2 - Mapping objectives to functional requirements

B.5 CS3 Functional requirements dependencies

875 Functional components possess dependencies which are stated requirements for the CS3 PP to include further components in support of the primary requirements.

876 To meet the evaluation requirements, it is necessary for all dependencies to be satisfied. Table B.3 below demonstrates how the dependencies of each included component have been satisfied.

877 All of the components of the CS3 PP are listed with a numeric line number. The dependencies of each component, if any, are listed alongside that component with a reference to the line number of the component which satisfies them. In the case of assurance component dependencies, all are satisfied hierarchically by assurance level EAL4, which is given as the reference. Component reference line numbers followed by '(H)' indicate that the dependency is satisfied by a hierarchical component to that referenced.

878 This table demonstrates that CS3 has no such unsatisfied dependencies.

Line Number	Component	Dependencies	Reference Line
1	FIA_ADA.3	FIA_ADP.1 FIA_UAU.1 FPT_TSA.2	2 11 60
2	FIA_ADP.1	FIA_UAU.1	11
3	FIA_ADP.2	FIA_UAU.1	11
4	FIA_AFL.2	FIA_UAU.1	11
5	FIA_ATA.1	ADV_FSP.1	EAL4
6	FIA_ATA.2	FIA_ATD.1 FPT_TSA.1	7 60 (H)
7	FIA_ATD.1	ADV_FSP.1	EAL4
8	FIA_ATD.2	ADV_FSP.1	EAL4
9	FIA_SOS.1	--	
10	FIA_SOS.2	--	
11	FIA_UAU.1	FIA_UID.1	14 (H)
12	FIA_UAU.6	FIA_UAU.1	11
13	FIA_UAU.9	FIA_UID.1 FPT_TSA.1	14 (H) 60 (H)
14	FIA_UID.2	FIA_ATD.2	8
15	FIA_USB.1	FIA_ATD.1 FDP_ACI.1 ADV_FSP.1	7 29 (H) EAL4
16	FTA_LSA.1	FIA_ATD.1 FTA_TAM.1	7 22

Table B.3 - CS3 functional component dependency analysis

Line Number	Component	Dependencies	Reference Line
17	FTA_MCS.2	FIA_UID.1 FPT_TSA.1	14 (H) 60 (H)
18	FTA_SSL.1 OR FTA_SSL.3	FTA_TAM.1 FIA_UAU.1	22 11
19	FTA_SSL.2	FTA_TAM.1 FIA_UAU.1	22 11
20	FTA_TAB.2	FTA_TAM.1	22
21	FTA_TAH.1	--	
22	FTA_TAM.1	FPT_TSA.1	60 (H)
23	FTA_TSE.1	FIA_ATD.1 FTA_TAM.1	7 22
24	FTP_TRP.1	--	
25	FDP_ACC.1	FDP_ACF.1	26
26	FDP_ACF.1	FDP_ACC.1	25
27	FDP_ACF.3	FDP_ACC.1	25
28	FDP_ACF.4	FDP_ACC.1	25
29	FDP_ACI.3	--	
30	FDP_RIP.2	--	
31	FDP_SAM.2	FPT_TSA.1 FDP_ACC.1	60 (H) 25
32	FDP_SAM.3	FDP_SAM.1 FDP_ACC.1	31 (H) 25
33	FDP_SAQ.1	FPT_TSA.1 FDP_ACC.1	60 (H) 25
34	FDP_SAQ.2	FDP_ACC.1	25
35	FAU_ARP.1	FAU_PAD.1 FAU_PIT.1 FAU_SAA.1 FPT_TSA.1	41 42 44 60 (H)
36	FAU_ARP.2	FAU_PAD.1 FAU_PIT.1 FAU_SAA.1	41 42 44
37	FAU_GEN.1	FIA_UID.1	14 (H)
38	FAU_GEN.2	FAU_GEN.1 FIA_UID.2	37 14
39	FAU_MGT.1	FAU_STG.1	49
40	FAU_MGT.3	--	
41	FAU_PAD.1	--	
42	FAU_PIT.1	--	

Table B.3 - CS3 functional component dependency analysis

Line Number	Component	Dependencies	Reference Line
43	FAU_PRO.2	FAU_STG.1 FPT_TSA.1	49 60 (H)
44	FAU_SAA.1	FAU_GEN.1	37
45	FAU_SAR.2	FAU_PRO.2 FAU_STG.1 FPT_TSA.1	43 49 60 (H)
46	FAU_SEL.1	FAU_GEN.1	37
47	FAU_SEL.2	FAU_SEL.1 FPT_TSA.1	46 60 (H)
48	FAU_SEL.3	FAU_SEL.1 FPT_TSA.1	46 60 (H)
49	FAU_STG.1	FAU_GEN.1	37
50	FAU_STG.3	FAU_GEN.1 FAU_STG.1	37 49
51	FPT_AMT.3	--	
52	FPT_FLS.1	ADV_FSP.2	EAL4
53	FPT_PHP.1	FPT_TSA.1 AGD_ADM.1	60 (H) EAL4
54	FPT_RCV.2	FPT_TSA.1 FPT_TST.1 ADV_FSP.2 AGD.ADM.1	60 (H) 62 (H) EAL4 EAL4
55	FPT_RVM.1	--	
56	FPT_SAE.1	--	
57	FPT_SEP.1	--	
58	FPT_SWM.1	--	
59	FPT_TDC.1	--	
60	FPT_TSA.2	FIA_ATA.1 FIA_ATD.1 FIA_UID.1	5 7 14 (H)
61	FPT_TSM.1	FPT_TSA.1	60 (H)
62	FPT_TST.3	FPT_AMT.3	51
63	FPT_TSU.1	FPT_TSA.1 AGD_ADM.1	60 (H) EAL4
64	FRU_RSA.1	FIA_UID.1	14 (H)

Table B.3 - CS3 functional component dependency analysis

B.6 CS3 Assurance requirements rationale

879 The assurance requirements for CS3 are portrayed in Table B.4 below. The rationale for the assurance requirements is stated following the table.

Requirement	Name
EAL4	Methodically Designed, Tested, and Reviewed
ALC_FLR.2	Flaw Reporting Procedures
ADO_DEL.2	Detection of Modification

Table B.4 - CS3 assurance requirements

B.6.1 Evaluation assurance level rationale

880 EAL4 - Methodically Designed, Tested and Reviewed.
This evaluation assurance level was selected as the fundamental set of assurance requirements for CS3, as it is designed to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices. EAL4 represents the highest practical level of assurance expected for a commercial grade product. EAL4 provides the greatest amount of assurance that commercial organisations may obtain without requiring substantial specialist knowledge, skills and other resources. As such, EAL4 appropriately supports the strong set of commercially-oriented functional requirements contained in CS3.

B.6.2 Assurance augmentations rationale

881 ALC_FLR.2 - Flaw Reporting Procedures.
In a high-end commercial product with the strong CS3 functional security requirements, it is necessary that, once installed properly, the TOE continue to operate in a secure state. Flaw remediation is important for commercial environments because it ensures that security flaws that are discovered by the product consumers will be tracked, corrected, and disseminated to the affected customers while the product is supported by the developer. ALC_FLR.2 provides the appropriate level of assurance for CS3 that the developer not only has basic flaw remediation procedures in effect but also has a procedure for accepting user reports of flaws and for providing flaw information and corrections to registered users. ALC_FLR.2 has a dependency upon AGD_ADM.1 - Administrator guidance, which is satisfied by EAL4 which includes that component.

882 ADO_DEL.2 - Detection of Modification.
In a high-end commercial product with the strong CS3 functional security requirements, there should be fundamental assurance that the TOE is delivered to the customer in a known secure state. The assurance gained by evaluation of the TOE must be maintained from the point of production to the point of secure installation and generation on the customer's premises, in order to provide satisfactory evidence that the TOE will begin operations securely. ADO_DEL.2 meets the first aspect of this need by ensuring that it is not possible to deliver to the customer without detection a modified copy of the evaluated master TOE. This assurance requirement provides that the developer will establish procedures for

delivery of the TOE to the customer, that technical measures are in place to detect modification of the TOE during delivery, and that it is possible to detect an unauthorised delivery. ADO_DEL.2 has a dependency upon ACM_CAP.2 - Authorisation Controls. That dependency is satisfied by EAL4 which includes the hierarchical component ACM_CAP.3.

Annex C

Rationale for PFFW Protection Profile

C.1 Introduction

883 This rationale material contributes to the evaluation evidence and is included as an
example of how such rationale might be presented.

884 Rationale would not normally be included in the published profile but should be
made available to profile users by the registration authorities as required.

885 As an aid to evaluation, it is divided into sections which parallel the APE assurance
class (see Part 3 of the CC). Readers and potential evaluators of this PP are invited
to comment upon the presentation, utility, and completeness of this material.

C.2 PFFW Security objectives

886 The CC requires that the security objectives are properly categorised as applied to
the firewall or its security environment, are useful and meaningful objectives, and
can be shown to cover all of the threats and policies identified.

887 No specific evidence is offered in support of any claims of utility of the stated
security objectives, the rationale aims to show that the objectives identified provide
a complete coverage of the threats and policies.

C.2.1 Threats to be addressed by the TOE

888 This section shows that a firewall (in its environment) which meets all of the stated
security objectives will effectively counter all of the identified threats. The term
'counter' is used without being categorical on the particular contribution of that
objective.

889 All non-IT security objectives (O.INSTALL, O.PACCESS, O.TRAIN) indirectly
support the countering of the threats as they are prerequisites for the firewall's
secure operation. In addition O.FLAW indirectly supports the countering of the
threats as it requires assurance (EAL) that gives confidence in the proper operation
of the security functions. Hence O.INSTALL, O.PACCESS, O.TRAIN, and
O.FLAW are not explicitly referenced in the elaboration of which objective
counters which threat. However, Table C.1 gives the full version of threats to
objectives mapping.

890 All secure usage assumptions (physical, personnel, connectivity) indirectly support
the countering of the threats as they are prerequisites for the firewall's secure
operation.

T.LACCESS An unauthorised person may gain logical access to the firewall.

891 O.ADMIN counters this threat as it requires the firewall design to only support direct console access. O.PROTECT counters this threat as it requires the firewall design to support a protection of the firewall executables and to protect other data necessary to enforce security (e.g., configuration data).

T.SPOOF An unauthorised person may carry out network address spoofing attacks (e.g., IP spoofing) from one network connection to another, traversing the firewall.

892 O.ACCESS counters this threat as it requires the information flow from source to destination address to be controlled. O.PROTECT counters this threat as it requires the firewall design to support a protection of the firewall executables and to protect other data necessary to enforce security (e.g., configuration data).

T.SACCESS An unauthorised person may carry out attacks on services.

893 O.ACCESS counters this threat as it requires the information flow from source to destination address to be controlled. O.PROTECT counters this threat as it requires the firewall design to support a protection of the firewall executables and to protect other data necessary to enforce security (e.g., configuration data).

T.SOURCE An unauthorised person may carry out source routing-type attacks at the network layer.

894 O.ACCESS counters this threat as it requires the information flow from source to destination address to be controlled. O.PROTECT counters this threat as it requires the firewall design to support a protection of the firewall executables and to protect other data necessary to enforce security (e.g., configuration data).

T.PENET An unauthorised person may carry out undetected penetration attempts.

895 O.AUDIT counters this threat as it requires the firewall to carry out auditing in order to hold the users accountable for their security relevant actions and to detect penetration attempts. Note that a machine user concept is applied. O.PROTECT counters this threat as it requires the firewall design to support a protection of the firewall executables and to protect other data necessary to enforce security (e.g., configuration data).

T.AUDITREV There may be lack of audit trail review.

896 O.AUDIT counters this threat as it requires a human understandable format of the audit trail and (minimum) review tools.

T.ACORR An attacker may corrupt the audit trail.

897 O.AUDIT counters this threat as it requires the firewall to carry out auditing in order to hold the users accountable for their security relevant actions and to detect penetration attempts. Note that a machine user concept is applied. O.PROTECT

counters this threat as it requires the firewall design to support a protection of the firewall executables and to protect other data necessary to enforce security (e.g., configuration data).

T.DCORR An attacker may modify the firewall configuration and other security-relevant data.

898 O.ADMIN counters this threat as it requires the firewall design to only support direct console access. O.AUDIT counters this threat as it requires the firewall to carry out auditing in order to hold the users accountable for their security relevant actions and to detect penetration attempts. Note that a machine user concept is applied. O.PROTECT counters this threat as it requires the firewall design to support a protection of the firewall executables and to protect other data necessary to enforce security (e.g., configuration data).

T.FLAW Security failures may occur because of flaws in the firewall.

899 O.FLAW counters this threat as it requires the firewall design to comply with the EAL specified in the assurance requirements section. It requires assurance that gives confidence in the proper operation of the security functions.

900 For additional information see Chapter 'C.2.2 Threats to be addressed by the operating environment' in the PP main body. The threats mentioned there must either be countered by the environment, procedural means, or accepted as potential system risks. Some of the non-IT objectives contribute to the minimisation of the residual risk.

901 The following table summarises the threats to security objectives mapping. Note that no special security policy is given for that PP.

Threats	Objectives	Policies
T.LACCESS	O.ADMIN, O.PROTECT, O.FLAW, O.INSTALL (E) ^a , O.PACCESS (E), O.TRAIN (E)	---
T.SPOOF	O.ACCESS, O.PROTECT, O.FLAW, O.INSTALL (E), O.PACCESS (E), O.TRAIN (E)	---

Table C.1 - Mapping of threats to security objectives

Threats	Objectives	Policies
T.SACCESS	O.ACCESS, O.PROTECT, O.FLAW, O.INSTALL (E), O.PACCESS (E), O.TRAIN (E)	---
T.SOURCE	O.ACCESS, O.PROTECT, O.FLAW, O.INSTALL (E), O.PACCESS (E), O.TRAIN (E)	---
T.PENET	O.AUDIT, O.PROTECT, O.FLAW, O.INSTALL (E), O.PACCESS (E), O.TRAIN (E)	---
T.AUDITREV	O.AUDIT, O.FLAW, O.INSTALL (E), O.PACCESS (E), O.TRAIN (E)	---
T.ACORR	O.AUDIT, O.PROTECT, O.FLAW, O.INSTALL (E), O.PACCESS (E), O.TRAIN (E)	---
T.DCORR	O.AUDIT, O.ADMIN, O.PROTECT, O.FLAW, O.INSTALL (E), O.PACCESS (E), O.TRAIN (E)	---
T.FLAW	O.FLAW, O.INSTALL (E), O.PACCESS (E), O.TRAIN (E)	---
T.EVIL_ADM (NC) ^b	O.TRAIN (E)	---
T.INSHARE (NC)	O.INSTALL (E)	---
T.INSTALL (NC)	O.INSTALL (E)	---
T.SERVICES (NC)	O.INSTALL (E)	---

Table C.1 - Mapping of threats to security objectives

- a. In the table (E) marks non-IT objectives.
- b. In the table (NC) marks threats not countered by the firewall, but partially addressed by non-IT objectives.

C.2.2 Threats to be addressed by the operating environment

902 This section shows that the threats to be countered by the operating environment of the firewall map to the security objectives identified for the environment. However, a certain residual risk remains, e.g. for reasons of design and scope limitations of the firewall (packet filter).

T.EVIL_ADM There are careless, wilfully negligent, or hostile system administration personnel.

903 O.TRAIN counters this threat as it requires the administration personnel to have an appropriate sense of responsibility and adequate technical skills.

T.INSHARE Hostile users on a protected network ("behind" the firewall) wish to share information with users on an external network.

904 O.INSTALL counters this threat as it requires the administration personnel to not only initiate the firewalls secure operation but also to maintain it. This includes user training and motivation. Furthermore the administrator can restrict the access from internal users to the outside world, which will limit the unintentional attempts. However, a strong intent to hostile sharing of information cannot be prevented as the firewall is not intended to examine the content of the packet.

T.INALL Hostile users on a protected network wish to attack machines that are part of the protected network.

905 O.INSTALL counters this threat for reasons of general user motivation improvement. However, a strong intent to hostile attacks within the internal network cannot be prevented as the firewall cannot place control over network traffic that does not pass the firewall itself.

T.SERVICES Hostile users try to carry out sophisticated attacks on higher-level protocols and services.

906 O.INSTALL counters this threat for reasons of general user motivation improvement. However, a strong intent to hostile attacks on higher levels of network protocols cannot be prevented as the firewall does not place control over higher levels of network protocols.

C.2.3 Policies to be addressed by the TOE

907 An organisational security policy could be based on all information that is available on the packet level, i.e. network addresses. However, the content of the packet is not intended to be examined. No special organisational security policy is given.

C.2.4 Completeness of the objectives

- 908 This chapter shows the mapping between IT objectives and associated threats.
- O.ACCESS** The firewall must provide controlled access between networks connected to it by permitting or denying the flow of packets.
- 909 This security objective is necessary to counter threats T.SPOOF, T.SACCESS, and T.SOURCE.
- O.ADMIN** The firewall must limit the direct access to it to a directly attached console.
- 910 This security objective is necessary to counter threats T.LACCESS and T.DCORR.
- O.PROTECT** The firewall must be able to separate data that it needs to operate (TSF data) from data that it is processing (packets).
- 911 This security objective is necessary to counter threats T.SPOOF, T.SACCESS, T.SOURCE, T.PENET, T.LACCESS, T.DCORR, and T.ACORR.
- O.AUDIT** The firewall must ensure that all users can subsequently be held accountable for their security relevant actions (see also O.ACCESS).
- 912 This security objective is necessary to counter threats T.PENET, T.AUDITREV, T.DCORR, and T.ACORR.
- O.FLAW** The firewall must be designed in order not to contain flaws in design or implementation.
- 913 This security objective is necessary to counter threats T.FLAW, T.PENET, T.DCORR, T.ACORR, T.SPOOF, T.SACCESS, T.SOURCE, T.AUDITREV, and T.LACCESS.
- O.PACCESS** Those responsible for the firewall must ensure that physical access to it is controlled.
- 914 This non-IT security objective is necessary to counter threats T.PENET, T.DCORR, T.ACORR, and T.LACCESS.
- O.TRAIN** Those responsible for the firewall must ensure that administrators have the necessary skills in establishment and maintenance of sound security policies and practices.
- 915 This non-IT security objective is necessary to counter the threat to be addressed by the operating environment T.EVIL_ADM. Note that dishonest human behaviour is outside the scope of the firewall.

O.INSTALL Those responsible for the firewall must ensure that it is delivered, installed, managed, and operated in a manner which maintains the system security.

916 This non-IT security objective is necessary to counter the threats to be addressed by the operating environment T.INSHARE, T.INALL, and T.SERVICES. Note that dishonest human behaviour is outside the scope of the firewall.

917 The following table summarises the security objectives to threats mapping. Note that no special security policy is given for that PP.

Objectives	Threats	Policies
O.ACCESS	T.SPOOF, T.SACCESS, T.SOURCE	---
O.ADMIN	T.LACCESS, T.DCORR	---
O.PROTECT	T.SPOOF, T.SACCESS, T.SOURCE, T.PENET, T.LACCESS, T.DCORR, T.ACORR	---
O.AUDIT	T.PENET, T.AUDITREV, T.DCORR, T.ACORR	---
O.FLAW	T.FLAW, T.SPOOF, T.SACCESS, T.SOURCE, T.PENET, T.LACCESS, T.DCORR, T.ACORR, T.AUDITREV	---
O.PACCESS (E) ^a	T.ACORR, T.DCORR, T.LACCESS, T.PENET	---
O.TRAIN (E)	T.EVIL_ADM (NC) ^b	---
O.INSTALL (E)	T.INSHARE (NC), T.INALL (NC), T.SERVICES (NC)	---

Table C.3 - Mapping of security objectives to threats

a. In the table (E) marks non-IT objectives.

b. In the table (NC) marks threats not countered by the firewall, but partially addressed by non-IT objectives.

918 The table above indicates that all objectives contribute to the ability of the firewall to counter a threat and that all threats have been addressed. Hence, there are no unnecessary objectives.

C.3 PFFW Functional requirements

919 The following table summarises the functional components included in this PP..

FAU_GEN.1	Audit Data Generation
FAU_MGT.1	Audit Trail Management
FAU_POP.1	Human Understandable Format
FAU_PRO.1	Restricted Audit Trail Access
FAU_SAR.1	Restricted Audit Review
FAU_SAR.3	Selectable Audit Review
FAU_STG.3	Prevention of Audit Data Loss
FIA_ADA.1	User Authentication Data Administration
FIA_ADP.1	Basic User Authentication Data Protection
FIA_ATA.1	User Attribute Initialisation
FIA_ATD.1	Shared User Attribute Definition
FIA_UAU.1	Basic User Authentication
FIA_UID.1	Basic User Identification
FIA_USB.1	User-Subject Binding
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
FPT_TSA.1	Basic Security Administration
FPT_TSM.1	Management Functions
FDP_ACC.2	Complete Object Access Control
FDP_ACF.2	Multiple Security Attribute Access Control
FDP_ACF.4	Access Authorisation and Denial
FDP_ACI.1	Static Attribute Initialisation
FDP_ETC.1	Export of User Data Without Security Attributes
FDP_ITC.1	Import of User Data Without Security Attributes
FDP_SAM.1	Administrator Attribute Modification
FDP_SAQ.1	Administrator Attribute Query

Table C.4 - Functional components included in this PP

FAU_GEN.1 Audit Data Generation

- 920 This component is included to directly support O.AUDIT as it requires the creation and maintenance of an audit trail.
- 921 For FAU_GEN.1.1 b) a minimum level of audit was selected.
- 922 For FAU_GEN.1.1 c) no other auditable events were assigned above the events indicated in the components. The table in the main body represented the specific events.
- 923 For FAU_GEN.1.2 a) the failure of an event was selected.
- 924 For FAU_GEN.1.2 b) no other auditable information was assigned. Therefore the complete item b) was removed from the requirements.
- 925 The component FAU_GEN.1 is dependent on FIA_UID.1. The dependency is resolved by the inclusion of FIA_UID.1.

FAU_MGT.1 Audit Trail Management

- 926 This component is included to directly support O.AUDIT as it requires the audit trail to be manageable by the administration personnel, e.g. by emptying the audit trail from time to time to avoid audit storage exhaustion. This component is included to directly support O.ADMIN and O.PROTECT as it requires appropriate firewall design that only allows direct access to the firewall via the directly attached console.
- 927 For FAU_MGT.1.1 create, delete, and empty the audit trail was selected.
- 928 The component FAU_MGT.1 is dependent on FAU_STG.1. The dependency is resolved by the inclusion of FAU_STG.3 which is hierarchical to FAU_STG.1 and satisfies the dependency.

FAU_POP.1 Human Understandable Format

- 929 This component is included to directly support O.AUDIT as it requires the audit trail to be understandable by the administration personnel.
- 930 The component FAU_POP.1 is dependent on FAU_STG.1. The dependency is resolved by the inclusion of FAU_STG.3 which is hierarchical to FAU_STG.1 and satisfies the dependency.

FAU_PRO.1 Restricted Audit Trail Access

- 931 This component is included to directly support O.AUDIT as it explicitly restricts access to the audit trail to authorised administrators. This component is included to directly support O.ADMIN and O.PROTECT as it requires appropriate firewall design that only allows direct access to the firewall via the directly attached console.

- 932 The component FAU_PRO.1 is dependent on FAU_STG.1 and FPT_TSA.1. The dependencies are resolved by the inclusion of FAU_STG.1 and FPT_TSA.1.

FAU_SAR.1 Restricted Audit Review

- 933 This component is included to directly support O.AUDIT as it requires tools for basic audit trail analysis. This component is included to directly support O.ADMIN and O.PROTECT as it requires appropriate firewall design that only allows direct access to the firewall via the directly attached console.

- 934 The component FAU_SAR.1 is dependent on FAU_STG.1, FPT_TSA.1, and FAU_PRO.1. The dependencies are resolved by the inclusion of FAU_STG.3, which is hierarchical to FAU_STG.1 and satisfies the dependency, FAU_TSA.1, and FPT_PRO.1.

FAU_SAR.3 Selectable Audit Review

- 935 This component is included to directly support O.AUDIT as it requires tools for improved audit trail analysis.

- 936 For FAU_SAR.3.1 the ST author is invited to assign criteria for searching and sorting the specific details of the firewall's audit trail.

- 937 The component FAU_SAR.3 is dependent on FAU_SAR.1. The dependency is resolved by the inclusion of FAU_SAR.1.

FAU_STG.3 Prevention of Audit Data Loss

- 938 This component is included to directly support O.AUDIT as it requires the audit trail to remain unaffected even in the case of audit storage exhaustion, firewall failure, and attack. Therefore O.FLAW is supported.

- 939 For FAU_STG.3.2 audit storage exhaustion, failure, and attack was selected.

- 940 For FAU_STG.3.3 the assignment is left for the ST author to execute. For the PP there is not a unique solution required.

- 941 The component FAU_STG.3 is dependent on FAU_GEN.1. The dependency is resolved by the inclusion of FAU_GEN.1.

FIA_ADA.1 User Authentication Data Administration

- 942 This component is included to directly support O.AUDIT as it requires user authentication attributes for the authorised administrator.

- 943 For FIA_ADA.1.1 a password mechanism was selected.

- 944 The component FIA_ADA.1 is dependent on FPT_TSA.1, FIA_ADP.1 and FIA_UAU.1. The dependencies are resolved by inclusion of FPT_TSA.1, FIA_ADP.1 and FIA_UAU.1.

FIA_ADP.1 Basic User Authentication Data Protection

- 945 This component is included to directly support O.AUDIT as it requires user authentication attributes to be protected.
- 946 The component FIA_ADA.1 is dependent on FIA_UAU.1. The dependency is resolved by inclusion of FIA_UAU.1.

FIA_ATA.1 User Attribute Initialisation

- 947 This component is included to directly support O.ACCESS as it requires initial values for attributes to enable access control on the packets traversing the firewall. These initial values are needed if, e.g. the attribute definition table of the firewall must be updated by the administration personnel or addresses of incoming packages are out of acceptable range.
- 948 The component FIA_ATA.1 is dependent on FIA_ATD.1 and FPT_TSA.1. The dependencies are resolved by the inclusion of FIA_ATD.1 and FPT_TSA.1.

FIA_ATD.1 Shared User Attribute Definition

- 949 This component is included to directly support O.AUDIT as it requires attributes for holding the (machine) users accountable. This component is included to directly support O.ACCESS as it requires attributes to enable access control on the packets traversing the firewall.
- 950 The definition of attributes for each user can only be applied in conjunction with the machine user concept or the authorised administrator user. Machine user attributes are referred to as network addresses or other appropriate attributes. The establishment and maintenance of a user to subject binding to hold a human user accountable for security relevant actions is outside the scope of the firewall (see also O.ACCESS).
- 951 However, the human users can only be held accountable for their security relevant actions if the subject identity recorded can be traced to a human user. The establishment and maintenance of such a user to subject binding is outside the scope of the firewall and must be carried out by the operating environment of the firewall.
- 952 The component FIA_ATD.1 is dependent on ADV_FSP.1. The dependency is resolved by the inclusion of an EAL.

FIA_UAU.1 Basic User Authentication

- 953 This component is included to directly support O.AUDIT as it provides authentication of the authorised administrator.
- 954 Since only authorised administrators will be authenticated, the word 'user' is refined to authorised administrator.

955 The component FIA_UAU.1 is dependent on FIA_UID.1. The dependency is resolved by the inclusion of FIA_UID.1.

FIA_UID.1 Basic User Identification

956 This component is included to directly support O.ACCESS as it requires attributes to enable access control on the packets traversing the firewall, and on identification of the authorised administrator.

957 The packet coming in is trivially identified by its network address or other appropriate attributes (machine user concept). There is a refinement from user to authorised administrator.

958 The component FIA_UID.1 is dependent on FIA_ATD.1. The dependency is resolved by the inclusion of FIA_ATD.1.

FPT_USB.1 User-Subject Binding

959 This component is included to directly support O.ACCESS since it allows each human user a separate subject to mediate access.

960 This component poses requirements for the association of the user security attributes with subjects. The FDP_ITC requirement is implementing part of this binding by providing some the relationship.

961 This component is dependent on FIA_ATD.1, ADV_FSP.1, and FDP_ACI.1. The dependencies are being resolved by the inclusion of FIA_ATD.1, FDP_ACI.1 and the inclusion of an EAL.

FPT_RVM.1 Non-Bypassability of the TSP

962 This component is included to directly support O.PROTECT as it requires appropriate firewall design that assures the security enforcing functions to always be invoked. The PP is not categorical about how this 'always invoked' property is designed. This component is important for the secure operation enforcement of the firewall.

963 The component FPT_RVM.1 has no dependencies.

FPT_SEP.1 TSF Domain Separation

964 This component is included to directly support O.PROTECT as it requires appropriate firewall design that clearly separates executables of the firewall and security relevant data from data which the firewall processes. This component is important for the secure operation enforcement of the firewall.

965 The component FPT_SEP.1 has no dependencies.

FPT_TSA.1 Basic Security Administration

966 This component is included to directly support O.ADMIN and O.PROTECT as it requires appropriate firewall design that clearly separates security relevant administrative functions from other functions and that only allows direct access to the firewall via the directly attached console. FPT_TSA.1.4 is trivially satisfied as the firewall does not offer any user services (see A.NO_USER).

967 For FPT_TSA.1.2 the services below are specified, which are directly related to the management of the PP requirements. As indicated in the operation an ST author might want to expand this list:

- a) administrator security attribute maintenance including default setup and overriding;
- b) audit function maintenance including start-up, shutdown;
- c) creation, deletion and emptying of audit trail;
- d) audit review tools;
- e) initialising user authentication data;
- f) modifying and display the firewall flow control parameters (access control parameters).

968 The component FPT_TSA.1 is dependent on FIA_UID.1, FIA_ATD.1, FIA_ATA.1, and AGD_ADM.1. The dependencies are resolved by the inclusion of FIA_UID.1, FIA_ATD.1, and FIA_ATA.1. The dependency on AGD_ADM.1 is resolved by the inclusion of an EAL.

FPT_TSM.1 Management Functions

969 This component is included to directly support O.ADMIN as it requires appropriate functions to handle the firewall securely. This component is included to directly support O.AUDIT as it requires auditing of configuration changes applied to the firewall.

970 For FPT_TSM.1.1 the TSF configuration parameters are specified, which are directly related to the management of the PP requirements. As indicated in the operation an ST author might want to expand this list:

- a) the access control parameters;
- b) default user attributes;
- c) default object attributes;
- d) audit rules;

e) [Assignment: others as specified by the ST author].

971 For FPT_TSM.1.2 the capabilities for the authorised administrator are specified, which are directly related to the management of the PP requirements. As indicated in the operation an ST author might want to expand this list:

- a) provide security attribute maintenance including default setup and overriding;
- b) manage the audit function including start-up, shutdown;
- c) provide creation, deletion and emptying of audit trail.
- d) review the audit data;
- e) initialise user authentication data;
- f) modify and display the firewall flow control parameters (access control parameters);
- g) manage interfaces;
- h) [Assignment: allow enabling and disabling of the set of peripheral devices specified by the ST author].

972 The component FPT_TSM.1 is dependent on FPT_TSA.1. The dependency is resolved by the inclusion of FPT_TSA.1.

FDP_ACC.2 Complete Object Access Control

973 This component is included to directly support O.ACCESS as it requires that all access to the objects (e.g., TCP/IP ports) will be mediated by the access control.

974 In FDP_ACC.2.1 the name of the access control SFP is provided: firewall flow policy.

975 In FDP_ACC.2.1 all subjects and all objects are covered under the firewall flow policy.

976 The component FDP_ACC.2 is dependent on FPT_ACF.1. The dependency is resolved by the inclusion of FPT_ACF.2 which is hierarchical to FDP_ACF.1 and satisfies the dependency.

FDP_ACF.2 Multiple Security Attribute Access Control

977 This component is included to directly support O.ACCESS as it provides the rules which shall be used to mediate the access between subjects and objects.

978 In FDP_ACF.2.1 the name of the access control SFP is provided: firewall flow policy.

979 In FDP_ACF.2.1 the attributes that are used in the access control rules are specified:

- 980 a) network identification of the subject and the object;
- 981 b) identity of the subject (e.g. TCP/IP address);
- 982 c) identity of the object (e.g. TCP/IP dress);
- 983 d) time.

984 In FDP_ACF.2.2 the actual access control rules are specified:

- a) If the time is between a period specified by the authorised administrator and
- b) either the subject or the object must have an internal network identification, and the other one must have an external network identification and
- c) the network associated with the subject (configuration parameter) must be equal to the network identification of the subject;
- d) access between the subject and object identity is explicitly allowed (which could be based on groups of subjects identities and object identities by the means of 'wildcards') and
- e) the access between the subject and object identity is not explicitly disallowed in a subset of the groups which allowed the operation (e.g. all users on a network are allowed to do action X, except all users whose port is located on number 25)

985 which ensures that access will only be granted at specified times, and the subject, if known, is on the right side of the network (this is required to counter masquerading of entities outside), and the firewall actually needs to forward (router function), and the access is allowed.

986 The component FDP_ACF.2 is dependent on FPT_ACC.1. The dependency is resolved by the inclusion of FPT_ACC.2 which is hierarchical to FDP_ACC.1 and satisfies the dependency.

FDP_ACF.4 Access Authorisation and Denial

987 This component is included to support O.ACCESS as it provides the authorised administrator the capability to manage the access control parameters (flow control access control parameters).

988 In FDP_ACF.4.1 the name of the access control SFP is provided: firewall flow policy.

989 The component FDP_ACF.4 is dependent on FPT_ACC.1. The dependency is resolved by the inclusion of FPT_ACC.2 which is hierarchical to FDP_ACC.1 and satisfies the dependency.

FDP_ACI.1 Static Attribute Initialisation

- 990 This component is included to directly support O.ACCESS as it allows secure default values for new objects.
- 991 In FDP_ACI.1.1 the name of the access control SFP is provided: firewall flow policy.
- 992 For FDP_ACI.1.1a restrictive default values is specified.
- 993 The component FDP_ACI.1 is dependent on FDP_ACF.1 or FDP_IFC.1. The dependency is resolved by the inclusion of FDP_ACF.2 which is hierarchical to FDP_ACF.1 and satisfies the dependency.

FDP_ETC.1 Export of User Data Without Security Attributes

- 994 This component is included to directly support O.ACCESS as it provides the requirements for the transmission of the packets.
- 995 In FDP_ETC.1.1 the name of the access control SFP is provided: firewall flow policy.
- 996 The component FDP_ETC.1 is dependent on FDP_ACC.1 or FDP_IFC.1. The dependency is resolved by the inclusion of FDP_ACC.2 which is hierarchical to FDP_ACC.1 and satisfies the dependency.

FDP_ITC.1 Import of User Data Without Security Attributes

- 997 This component is included to directly support O.ACCESS as it provides the requirements for the reception of the packets.
- 998 In FDP_ITC.1.1 the name of the access control SFP is provided: firewall flow policy.
- 999 For FDP_ITC.1.4 the rules being followed while importing packets are described. These rules specify: the user identity, the object identity, the subject network, and the object network.
- 1000 The component FDP_ICT.1 is dependent on FDP_ACC.1 or FDP_IFC.1. The dependency is resolved by the inclusion of FDP_ACC.2 which is hierarchical to FDP_ACC.1 and satisfies the dependency.

FDP_SAM.1 Administrator Attribute Modification

- 1001 This component is included to directly O.ACCESS as it provides the authorised administrator with the capability to modify the attributes.
- 1002 In FDP_SAM.1.1 the name of the access control SFP is provided: firewall flow policy.

1003 For FDP_SAM.1.1 the ST author is invited to specify the parameters the authorised administrator can modify.

1004 The component FDP_SAM.1 is dependent on FDP_ACC.1 or FDP_IFC.1 and FDP_TSA.1. The dependency is resolved by the inclusion of FDP_ACC.2 which is hierarchical to FDP_ACC.1 and satisfies the dependency and the inclusion of FDP_TSA.1

FDP_SAQ.1 Administrator Attribute Query

1005 This component is included to directly O.ACCESS as it provides the authorised administrator with the capability to request the attributes.

1006 In FDP_SAQ.1.1 the name of the access control SFP is provided: firewall flow policy.

1007 For FDP_SAQ.1.1 the ST author is invited to specify the attributes the authorised administrator can review.

1008 The component FDP_SAQ.1 is dependent on FDP_ACC.1 or FDP_IFC.1 and FDP_IFC.1. The dependency is resolved by the inclusion of FDP_ACC.2 which is hierarchical to FDP_ACC.1 and satisfies the dependency and the inclusion of FDP_TSA.1

C.4 PFFW Assurance requirements

1009 The assurance requirements consist of EAL1 - functionally tested.

1010 The intent of this PP is to specify assurance requirements that can easily be met by most of the commercially available packet filter firewalls. Even EAL1 gives the firewall user considerable additional confidence beyond developer assertion in the firewall's secure operation. As the firewall only covers the packet level of information flow and does not regard higher protocol layers the cost to benefit ratio would not support a high assurance EAL.

1011 The assurance level EAL1 is included to directly support O.FLAW as it requires testing in order to assure that the firewall behaves as specified in the guidance documentation.

Annex D

CC observation report (CCOR)

D.1 Introduction

- 1012 The CC sponsoring organisations welcome feedback from the community and are particularly interested in observations and comments arising out of trial application of the criteria.
- 1013 The CC sponsoring organisations have set up a body, the Common Criteria Implementation Board (CCIB), to coordinate and learn from the community experience and to ensure that future issues of the CC can benefit from that experience.
- 1014 Comments, observations, and requests for interpretations should be sent to one of the addresses listed inside the front cover of the CC. If you require feedback on a specific evaluation matter, you should use the contact address which corresponds to the evaluation authority concerned.

D.2 Categorisation of observation report

- 1015 In order to allow automated categorisation of the observations, a standard observation format is needed. Each observation should include an identifier as to whether the comment pertains to the **approach** in the CC, the technical **detail** of any specific portion of the CC, or **editorial** work that needs to be done. Additionally, for comments on technical detail, an indication of the scope of the comment (e.g., **local**, **global**) should be provided.
- 1016 The following provides a description of each of these terms:
- a) *Approach*: observations requesting further guidance relating to the approach of the CC which the author of the observation report considers to be fundamental to the further progress of the CC or trial application of the criteria should be marked with this identifier.
 - b) *Detail*: Specific observations on technical details of the CC should be marked with this identifier. These comments should be further categorised as either local or global.
- Local*: is applicable to a single specific class, family, component, or element.
- Global*: is applicable to multiple classes, families, components, or elements.

- c) *Editorial*: typographical and grammatical errors, as well as comments on presentation style.

Local: is applicable to a single specific class, family, component, or element.

Global: is applicable to multiple classes, families, components, or elements.

D.3 Format of observation report

1017 The following provides a description of each of the structure of the required comment format and an example of a comment in the required format.

1018 If you are submitting one or more observations by electronic mail or other machine readable format, please insert the tags defined below starting in the first column as this will greatly assist in any automated handling of your input.

1019 Each observation report should consist of three parts.

- a) The first part consists of a tags **\$1:** to **\$4:**, which includes the information to allow the unique identification of the originator. This first set of tags is required only once per single observation or batch of observations.

- b) The second part consists of tags **\$5:** to **\$9:**, which includes the information to allow the unique identification and categorisation of the observation, the actual observation itself and suggested solution. The text of each observation should extend to as many lines as are needed to fully express the observation. There can be one or more observations in an observation report.

The set of tags **\$5:** to **\$9:**, comprising this second part of the observation report, should be repeated for each observation being submitted.

- c) The third part consists of a single terminating tag **\$\$:**. This final tag is required only once per single observation or batch of observations.

D.3.1 Tag definitions for observation report

\$1: Originator name

1020 Name of commenter (only required once per message).

\$2: Originator organisation

1021 Originator organisation/affiliation (only required once per message).

\$3: Return address

1022 Electronic mail or other address for response (only required once per message).

\$4: Date

1023 Submission date of observation YY/MM/DD (only required once per message).

\$5: Originator report reference identification

1024 Reference for observation which is unique to originator. Please include your initials or similar unique discriminator, e.g., ABC1234.

\$6: One line summary/title of observation

1025 Short summary/title for problem (up to 60 characters).

\$7: CC document reference

1026 Single reference to the affected area of the CC as detailed as appropriate. Where possible, part number, section, paragraph, class, family, component, or requirement reference should be provided.

1027 The template for CC document reference is as follows:

\$7: Part / Section / Paragraph / [Approach / Detail - [Local / Global] / Editorial] - [Local / Global] / [Keyword]

1028 The CC document reference template should be completed as follows (see below for completed example):

- a) The characters “\$7:”, to indicate the start of an observation.
- b) Identification of the CC part, section, and paragraph to which the comment applies in the CC. All 3 pieces of identifying information should be provided, each separated by a slash character (/).

Valid identifiers for the CC Part are e.g., part 1 or 1, part 2 or 2, part 3 or 3, and profiles or PP.

Identification for the CC section should be either a section number (e.g., 1.3.2), if applicable, or, for requirement classes, families, or components, the name of the class (e.g., FIA), family (e.g., FIA_ATD), or component (e.g., FIA_ATD.1).

- c) Identification of the reviewer’s categorisation of the observation. Brackets “[.]” indicate that the reviewer should choose *one* of the options contained within the brackets, these can be abbreviated to the initial character only (e.g., “A”, “D - L”, or “E - G”).
- d) An optional keyword.

1029 Any identification field should be left blank or be filled with an asterisk (*) to indicate that the field is not applicable or necessary for the comment.

\$8: Statement of observation

1030 Comprehensive statement of observation or query, contains the actual text of the observation. Should include specific reference to examples of the observation, where appropriate.

\$9: Suggested solution

1031 Proposed solution or solution approach.

\$\$: Terminating tag.

1032 This enables any automated handling to determine the end of the batch of observations (only required once per batch of observations).

D.3.2 Example observations:

\$1: A. N. Other

\$2: PPs 'R' US

\$3: another@ppsrus.com

\$4: 960131

\$5: ano.comment.1

\$6: Presentation comment.

\$7: 1 / 8.1 / 90 / Editorial - Local /

\$8: The word "global" at the end of the first line should be italicised.

\$9: Italicise "global".

\$5: ano.comment.2

\$6: Missing requirement for audit.

\$7: 2 / FAU / 336 / Detail - Local /

\$8: The first sentence of this paragraph is incomplete.

\$9: The first sentence should include "imminent" violations.

\$5: ano.comment.3

\$6: Problems in navigating the document.

\$7: 2 / * / * / Approach / threats

\$8: The statements of threat in the functional families are largely re-statements of the family behaviour from the threat viewpoint. Does this material need to be re-stated twice within the functional families?

\$9: Could all threat information be described in a separate section with a table mapping the various functional components to the threats they address?

\$\$: This is the end tag, the contents are immaterial.

D.4 Printed observation report

1033 An example of a printed observation report is provided in Table D.1.

COMMON CRITERIA OBSERVATION REPORT	
\$1:	Originator Name
\$2:	Originator organisation
\$3:	Return address
\$4:	Date
\$5:	Originator report reference identification
\$6:	One line summary/title of observation
\$7:	CC document reference
\$8:	Statement of observation
\$9:	Suggested solution
\$\$:	

Table D.1 - CC observation report